Lecture Notes in Computer Science 4341

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

David Hutchison
Lancaster University, UK

Takeo Kanade
Carnegie Mellon University, Pittsburgh, PA, USA

Josef Kittler
University of Surrey, Guildford, UK

Jon M. Kleinberg
Cornell University, Ithaca, NY, USA

Friedemann Mattern
ETH Zurich, Switzerland

John C. Mitchell
Stanford University, CA, USA

Moni Naor
Weizmann Institute of Science, Rehovot, Israel

Oscar Nierstrasz
University of Bern, Switzerland

C. Pandu Rangan
Indian Institute of Technology, Madras, India

Bernhard Steffen
University of Dortmund, Germany

Madhu Sudan
Massachusetts Institute of Technology, MA, USA

Demetri Terzopoulos
University of California, Los Angeles, CA, USA

Doug Tygar
University of California, Berkeley, CA, USA

Moshe Y. Vardi
Rice University, Houston, TX, USA

Gerhard Weikum
Max-Planck Institute of Computer Science, Saarbruecken, Germany

Phong Q. Nguyen (Ed.)

Progress in Cryptology – VIETCRYPT 2006

First International Conference on Cryptology in Vietnam
Hanoi, Vietnam, September 25-28, 2006
Revised Selected Papers

Volume Editor

Phong Q. Nguyen
Ecole Normale Supérieure
Département d'Informatique
45, rue d'Ulm, 75230 Paris Cedex 05, France
E-mail: Phong.Nguyen@ens.fr

Library of Congress Control Number: 2006938421

CR Subject Classification (1998): E.3, G.2.1, D.4.6, K.6.5, K.4, F.2.1-2, C.2

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743
ISBN-10 3-540-68799-8 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-68799-3 Springer 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. Violations are liable to prosecution under the German Copyright Law.

Springer is a part of Springer Science+Business Media

springer.com

© Springer-Verlag Berlin Heidelberg 2006
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 11958239 06/3142 5 4 3 2 1 0

Preface

These are the proceedings of VIETCRYPT 2006, the first international conference on cryptology hosted in Vietnam. The conference was organized by FPT Software, in cooperation with Vietnam's Institute of Mathematics. It was held in the beautiful city of Hanoi, September 25–28, 2006. This conference would certainly not have been possible without Phan Dinh Dieu, the General Chair. I also wish to thank Nguyen Quoc Khanh, Nguyen Duy Lan and Phan Duong Hieu for their invaluable help in organizing the conference.

The Program Committee, consisting of 36 members from 17 countries, considered 78 papers (from 19 countries) and selected 24 for presentation. These proceedings include the revised versions of the 24 papers accepted by the Program Committee. These papers were selected from all the anonymous submissions to the conference on the basis of originality, quality and relevance to cryptography. Revisions were not checked and the authors bear full responsibility for the contents of their papers. The conference program also included two invited talks: it was a great honor to have Tatsuaki Okamoto and Jacques Stern as invited speakers. Their talks were entitled, respectively, "On Pairing-Based Cryptosystems" and "Cryptography in Financial Transactions: Current Practice and Future Directions."

The selection of papers was a difficult and challenging task. Each submission was reviewed by at least three referees. I wish to thank the Program Committee members, who did an excellent job, and devoted much effort and valuable time to read and select the papers. In addition, I gratefully acknowledge the help of a large number of colleagues who reviewed submissions in their areas of expertise. They are all listed here and I apologize for any inadvertent omission. I also wish to thank Springer for publishing the proceedings in the *Lecture Notes in Computer Science* series.

All paper submissions to VIETCRYPT 2006 were handled electronically, using the amazing iChair software developed at the École Polytechnique Fédérale de Lausanne (EPFL) by Thomas Baignères and Matthieu Finiasz. I also wish to thank Jacques Beigbeder for installing iChair at the ENS.

Finally, I would like to thank all the authors who submitted papers.

October 2006 Nguyễn Phong Quang

VIETCRYPT 2006

International Conference on Cryptology in Vietnam

September 25 – 28, 2006, Hanoi, Vietnam

Organized by

FPT Software

in cooperation with

Vietnam's Institute of Mathematics

Organization Committee

Nguyen Quoc Khanh ..... FPT Software, Vietnam
Nguyen Lam Phuong ..... FPT Software, Vietnam - Chair
Phan Van Hoa ..... FPT Software, Vietnam

General Chair

Phan Dinh Dieu, Vietnam National University, Vietnam

Program Chair

Nguyen Phong Quang, École Normale Supérieure and CNRS, France

Program Committee

Masayuki Abe ..... NTT Information Sharing Platform Laboratories, Japan
Feng Bao ..... Institute for Infocomm Research, Singapore
Alex Biryukov ..... University of Luxembourg, Luxembourg
Daniel Bleichenbacher ..... Switzerland
Xavier Boyen ..... Voltage, USA
Jung Hee Cheon ..... Seoul National University, South Korea
Ed Dawson ..... Queensland University of Technology, Australia
Marc Fischlin ..... Technische Universität Darmstadt, Germany
Craig Gentry ..... Stanford University, USA
Ha Huy Khoai ..... Institute of Mathematics, Vietnam
Shai Halevi ..... IBM Research, USA
Antoine Joux ..... DGA and University of Versailles, France
Pascal Junod ..... Nagravision, Switzerland
Jonathan Katz ..... University of Maryland, USA
Kwangjo Kim ..... Information and Communications University, South Korea

Lars Knudsen ..... Technical University of Denmark, Denmark
Neal Koblitz ..... University of Washington, USA
Kaoru Kurosawa ..... Ibaraki University, Japan
Arjen K. Lenstra ..... EPFL, Switzerland
Ilya Mironov ..... Microsoft Research, USA
Chanathip Namprempre ..... Thammasat University, Thailand
Mats Naslund ..... Ericsson, Sweden
Nguyen Duy Lan ..... CSIRO ICT Centre, Australia
Nguyen Quoc Khanh ..... FPT Corporation, Vietnam
Kazuo Ohta ..... University of Electro-Communications, Japan
Pascal Paillier ..... Gemalto, France
Kenny Paterson ..... Royal Holloway University of London, UK
Phan Duong Hieu ..... University College London, UK
Bart Preneel ..... Katholieke Universiteit Leuven, Belgium
C. Pandu Rangan ..... IIT Madras, India
Matt Robshaw ..... France Telecom R&D, France
Phil Rogaway ..... UC Davis, USA and Chiang Mai University, Thailand
Nigel Smart ..... University of Bristol, UK
Mike Szydlo ..... RSA, USA
Tsuyoshi Takagi ..... Future University, Japan
Xiaoyun Wang ..... Tsinghua University, China

External Reviewers

Michel Abdalla
Joosang Baek
Colin Boyd
Reinier Broker
Michael Cheng
Sherman Chow
Yvonne Cliff
Matthez Dailey
Jintai Ding
Ratna Dutta
Jean-Charles Faugère
Rosario Gennaro
Rob Granger
Yoshikazu Hanatani
Matt Henricksen
Mattias Johansson
Yutaka Kawai
Phongsak Keeratiwintakorn
Yuuichi Kokubun
Yuichi Komano
Nam-Seok Kwak
Reynald Lercier
Joseph Liu
Daegun Ma
Alexander May
Satoshi Miyagawa
Kunihiko Miyazaki
Sourav Mukhopadhyay
Dang Nguyen Duc
Karl Norrman
DaeHun Nyang
Miyako Ohkubo
Seiji Okuaki
Dag Arne Osvik
Dan Page
Kun Peng
Duong Quang Viet
Vincent Rijmen
Peter Ryan
Bagus Santoso
Dong-Gyu Seon
Ji Sun Shin
Masaaki Shirase
Isamu Teranishi
Soren Steffen Thomsen
Dongvu Tonien
Pim Tuyls
Frederik Vercauteren
Charlotte Vikkelsoe
Duc Liem Vo
David Woodruff
Yongdong Wu
Kazuki Yoneyama
Eun Sun Yoo
HyoJin Yoon

Table of Contents

Ring Signatures and Group Signatures

Hash Functions

Cryptanalysis

Key Agreement and Threshold Cryptography

Public-Key Encryption