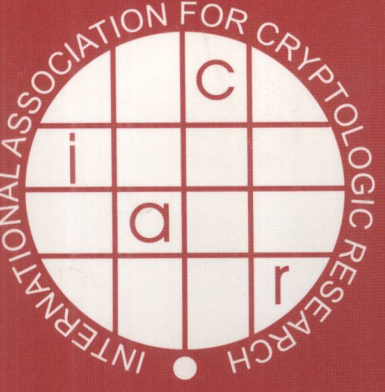
Louis Goubin
Mitsuru Matsui (Eds.)

LNCS 4249

Cryptographic Hardware and Embedded Systems – CHES 2006

8th International Workshop
Yokohama, Japan, October 2006
Proceedings



Springer

TP309-53
C524
2006

Louis Goubin Mitsuru Matsui (Eds.)

Cryptographic Hardware and Embedded Systems – CHES 2006

8th International Workshop
Yokohama, Japan, October 10-13, 2006
Proceedings

Springer

Volume Editors

Louis Goubin
PRiSM Laboratory, Versailles St.-Quentin-en-Yvelines University
45 avenue des États-Unis, 78035 Versailles, France
E-mail: louis.goubin@prism.uvsq.fr

Mitsuru Matsui
Mitsubishi Electric Corporation, Information Technology R&D Center
5-1-1 Ofuna Kamakura, Kanagawa 247-8501, Japan
E-mail: matsui.mitsuru@ab.mitsubishielectric.co.jp

Library of Congress Control Number: 2006933431

CR Subject Classification (1998): E.3, C.2, C.3, B.7, G.2.1, D.4.6, K.6.5, F.2.1, J.2

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743
ISBN-10 3-540-46559-6 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-46559-1 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: 11894063 06/3142 5 4 3 2 1 0

Lecture Notes in Computer Science 4249

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

Preface

These are the proceedings of the Eighth Workshop on Cryptographic Hardware and Embedded Systems (CHES 2006) held in Yokohama, Japan, October 10-13, 2006. The CHES workshop has been sponsored by the International Association for Cryptographic Research (IACR) since 2004. The first and the second CHES workshops were held in Worcester in 1999 and 2000, respectively, followed by Paris in 2001, San Francisco Bay Area in 2002, Cologne in 2003, Boston in 2004 and Edinburgh in 2005. This is the first CHES workshop held in Asia.

This year, a total of 112 paper submissions were received. The review process was therefore a delicate and challenging task for the Program Committee members. Each paper was carefully read by at least three reviewers, and submissions with a Program Committee member as a (co-)author by at least five reviewers. The review process concluded with a two week Web discussion process which resulted in 32 papers being selected for presentation. Unfortunately, there were a number of good papers that could not be included in the program due to a lack of space. We would like to thank all the authors who submitted papers to CHES 2006.

In addition to regular presentations, we were very fortunate to have in the program three excellent invited talks given by Kazumaro Aoki (NTT) on "Integer Factoring Utilizing PC Cluster," Ari Juels (RSA Labs) on "The Outer Limits of RFID Security" and Ahmad Sadeghi (Ruhr University Bochum) on "Challenges for Trusted Computing." The program also included a rump session, chaired by Christof Paar, featuring informal presentations on recent results.

We are very grateful to the Program Committee members and to the external reviewers for their hard work. Special thanks are also due to the members of the Local Committee: Akashi Satoh (Secretary - IBM Japan Ltd.), Toru Akishita (Sony Corporation), Tetsuya Izu (Fujitsu Laboratories Ltd.), Masanobu Koike (Toshiba Solutions Corporation), Natsume Matsuzaki (Matsushita Electric Industrial Co., Ltd.), Shiho Moriai (Sony Computer Entertainment Inc.), Sumio Morioka (NEC Corporation), Hanae Nozaki (Toshiba Corporation), Kenji Ohkuma (IPA), Katsuyuki Okeya (Hitachi Ltd.), Shunsuke Ota (Hitachi Ltd.), Yasuyuki Sakai (Mitsubishi Electric Corporation), Junji Shikata (Yokohama National University), Daisuke Suzuki (Mitsubishi Electric Corporation), Yukiyasu Tsunoo (NEC Corporation), Takanari Ueno (IPA), Takashi Watanabe (Hitachi Ltd.) and Atsuhiro Yamagishi (IPA), for their strong support.

Special thanks go to Tsutomu Matsumoto, the General Chair and local organizer for his extensive efforts to bring the workshop to the beautiful historic city of Yokohama, Japan. The Publicity Chair Çetin Kaya Koç was always very helpful and patient at all stages of the organization. Jens-Peter Kaps helped us as our dedicated webmaster for maintaining the Web review system.

此为试读,需要完整PDF请访问: www.ertongbook.com

We would also thank the corporate financial supporters, Cryptography Research, Inc., RSA Security Japan Ltd., Fujitsu Limited, IBM Corporation, Information Technology Promotion Agency, Japan (IPA), Initiative for Research on Information Security, Mitsubishi Electric Corporation, NTT Corporation, Renesas Technology Corp., Toshiba Corporation and Yokohama National University. Obviously CHES2006 was not possible without these supporters.

Lastly we would like to thank the CHES Steering Committee members for their hearty support and for giving us the honor of serving at such a prestigious conference.

October 2006

Louis Goubin
Mitsuru Matsui

8th Workshop on Cryptographic Hardware and Embedded Systems

October 10 – 13, 2006, Yokohama, Japan
http://www.chesworkshop.org/

Organizing Committee

- Tsutomu Matsumoto (General Chair), Yokohama National University, Japan
- Çetin Kaya Koç (Publicity Chair), Oregon State University, USA
- Louis Goubin (Program Co-chair), Versailles St-Quentin-en-Yvelines University, France
- Mitsuru Matsui (Program Co-chair), Mitsubishi Electric Corporation, Japan

Program Committee

- Mehdi-Laurent Akkar, Texas Instruments, France
- Jean-Sébastien Coron, University of Luxembourg, Luxembourg
- Nicolas T. Courtois, Gemalto, France
- Joan Daemen, ST Microelectronics, Belgium
- Pierre-Alain Fouque, ENS, Paris, France
- Jim Goodman, ATI Technologies, Canada
- Helena Handschuh, Spansion, France
- Tetsuya Izu, Fujitsu Laboratories Ltd., Japan
- Marc Joye, Thomson R&D, France
- Seungjoo Kim, Sungkyunkwan University, South Korea
- Çetin Kaya Koç, Oregon State University, USA
- Pil Joong Lee, Postech, South Korea
- Frédéric Muller, HSBC, France
- Katsuyuki Okeya, Hitachi, Japan
- Elisabeth Oswald, Graz University of Technology, Austria
- Christof Paar, Ruhr-Universität Bochum, Germany
- Josyula R. Rao, IBM T.J. Watson Research Center, USA
- Erkay Savaş, Sabanci University, Turkey
- Werner Schindler, Bundesamt für Sicherheit in der Informationstechnik, Germany
- Nigel Smart, University of Bristol, UK
- François-Xavier Standaert, Université Catholique de Louvain-la-Neuve, Belgium
- Berk Sunar, Worcester Polytechnic Institute, USA
- Frédéric Valette, DGA/CELAR, France
- Ingrid Verbauwhede, Katholieke Universiteit Leuven, Belgium
- Colin Walter, Comodo CA, UK
- Sung-Ming Yen, National Central University, Taiwan

Steering Committee

- Marc Joye, Thomson R&D, France
- Çetin Kaya Koç, Oregon State University, USA
- Christof Paar, Ruhr-Universität Bochum, Germany
- Jean-Jacques Quisquater, Université Catholique de Louvain, Belgium
- Josyula R. Rao, IBM T.J. Watson Research Center, USA
- Berk Sunar, Worcester Polytechnic Institute, USA
- Colin D. Walter, Comodo Research Lab, UK

External Referees

- Onur Acıiçmez
- Manfred Aigner
- Toru Akishita
- Frédéric Amiel
- Cédric Archambeau
- Lejla Batina
- Kamel Bentahar
- Guido Bertoni
- Régis Bévan
- Arnaud Boscher
- Donald R. Brown
- Cécile Canovas
- Chien-Ning Chen
- Benoît Chevallier-Mames
- Jessy Clédière
- Eric Dahmen
- Yasin Demirbas
- Loïc Duflot
- Takashi Endo
- Pooya Farshim
- Benoît Feix
- Kris Gaj
- Christophe Giraud
- Aline Gouget
- Rob Granger
- Johann Großschädl
- Jorge Guajardo
- Frank Guerkaynak
- Tim Güneysu
- Adnan Gutub
- DongGuk Han
- Christoph Herbst
- Yong Ho Hwang
- Kouichi Itoh
- Tetsuya Izu
- Charanjit Jutla
- Jin Ho Kim
- Tae Hyun Kim
- Young Hwan Kim
- Thorsten Kleinjung
- Sandeep Kumar
- Noboru Kunihiro
- Sébastien Kunz-Jacques
- Eun Jeong Kwon
- Soonhak Kwon
- Kerstin Lemke-Rust
- Wei-Chih Lien
- Manfred Lochter
- François Macé
- Pascal Manet
- Stefan Mangard
- Marian Margraf
- Gwenaëlle Martinet
- John McNeill
- Nele Mentens
- Guerric Meurice de Dormale
- Andrew Moss
- Francis Olivier
- Berna Örs
- Dan Page
- Jung Hyung Park
- Fabrice Pautot
- Eric Peeters
- Jan Pelzl
- Thomas Peyrin
- Thomas Popp
- Axel Poschmann
- Emmanuel Prouff
- Jean-Luc Rainard
- Arash Reyhani-Masoleh
- Francisco Rodriguez-Henriquez
- Kazuo Sakiyama
- Gökay Saldamlı
- Akashi Satoh
- Sven Schäge
- Daniel Schepers
- Kai Schramm
- Jae Woo Seo
- Jong Hoon Shin
- Alexei Tchoulkine
- Alexandre F. Tenca
- Stefan Tillich
- Elena Trichina
- Pim Tuyls
- François Vacherand
- Camille Vuillaume
- Takashi Watanabe
- Jun Yajima
- Yeon Hyeong Yang
- Hirotaka Yoshida
- Masayuki Yoshino
- Dae Hyun Yum

Previous CHES Workshop Proceedings

- **CHES 1999:** Çetin K. Koç and Christof Paar (Editors). *Cryptographic Hardware and Embedded Systems*, vol. 1717 of *Lecture Notes in Computer Science*, Springer, 1999.
- **CHES 2000:** Çetin K. Koç and Christof Paar (Editors). *Cryptographic Hardware and Embedded Systems*, vol. 1965 of *Lecture Notes in Computer Science*, Springer, 2000.
- **CHES 2001:** Çetin K. Koç, David Naccache, and Christof Paar (Editors). *Cryptographic Hardware and Embedded Systems*, vol. 2162 of *Lecture Notes in Computer Science*, Springer, 2001.
- **CHES 2002:** Burton S. Kaliski, Çetin K. Koç, and Christof Paar (Editors). *Cryptographic Hardware and Embedded Systems*, vol. 2523 of *Lecture Notes in Computer Science*, Springer, 2002.
- **CHES 2003:** Colin D. Walter, Çetin K. Koç, and Christof Paar (Editors). *Cryptographic Hardware and Embedded Systems*, vol. 2779 of *Lecture Notes in Computer Science*, Springer, 2003.
- **CHES 2004:** Marc Joye and Jean-Jacques Quisquater (Editors). *Cryptographic Hardware and Embedded Systems*, vol. 3156 of *Lecture Notes in Computer Science*, Springer, 2004.
- **CHES 2005:** Josyula R. Rao and Berk Sunar (Editors). *Cryptographic Hardware and Embedded Systems*, vol. 3659 of *Lecture Notes in Computer Science*, Springer, 2005.

Lecture Notes in Computer Science

For information about Vols. 1–4144

please contact your bookseller or Springer

Vol. 4249: L. Goubin, M. Matsui (Eds.), Cryptographic Hardware and Embedded Systems - CHES 2006. XIV, 462 pages. 2006.

Vol. 4248: S. Staab, V. Svátek (Eds.), Engineering Knowledge in the Age of the Semantic Web. XIV, 400 pages. 2006. (Sublibrary LNAI).

Vol. 4243: T. Yakhno, E. Neuhold (Eds.), Advances in Information Systems. XV, 420 pages. 2006.

Vol. 4241: R. Beichel, M. Sonka (Eds.), Computer Vision Approaches to Medical Image Analysis. XI, 262 pages. 2006.

Vol. 4239: H.Y. Youn, M. Kim, H. Morikawa (Eds.), Ubiquitous Computing Systems. XVI, 548 pages. 2006.

Vol. 4238: Y.-T. Kim, M. Takano (Eds.), Management of Convergence Networks and Services. XVIII, 605 pages. 2006.

Vol. 4229: E. Najm, J.F. Pradat-Peyre, V.V. Donzeau-Gouge (Eds.), Formal Techniques for Networked and Distributed Systems - FORTE 2006. X, 486 pages. 2006.

Vol. 4228: D.E. Lightfoot, C.A. Szyperski (Eds.), Modular Programming Languages. X, 415 pages. 2006.

Vol. 4227: W. Nejdl, K. Tochtermann (Eds.), Innovative Approaches for Learning and Knowledge Sharing. XVII, 721 pages. 2006.

Vol. 4224: E. Corchado, H. Yin, V. Botti, C. Fyfe (Eds.), Intelligent Data Engineering and Automated Learning – IDEAL 2006. XXVII, 1447 pages. 2006.

Vol. 4223: L. Wang, L. Jiao, G. Shi, X. Li, J. Liu (Eds.), Fuzzy Systems and Knowledge Discovery. XXVIII, 1335 pages. 2006. (Sublibrary LNAI).

Vol. 4222: L. Jiao, L. Wang, X. Gao, J. Liu, F. Wu (Eds.), Advances in Natural Computation, Part II. XLII, 998 pages. 2006.

Vol. 4221: L. Jiao, L. Wang, X. Gao, J. Liu, F. Wu (Eds.), Advances in Natural Computation, Part I. XLI, 992 pages. 2006.

Vol. 4219: D. Zamboni, C. Kruegel (Eds.), Recent Advances in Intrusion Detection. XII, 331 pages. 2006.

Vol. 4217: P. Cuenca, L. Orozco-Barbosa (Eds.), Personal Wireless Communications. XV, 532 pages. 2006.

Vol. 4216: M.R. Berthold, R. Glen, I. Fischer (Eds.), Computational Life Sciences II. XIII, 269 pages. 2006. (Sublibrary LNBI).

Vol. 4213: J. Fürnkranz, T. Scheffer, M. Spiliopoulou (Eds.), Knowledge Discovery in Databases: PKDD 2006. XXII, 660 pages. 2006. (Sublibrary LNAI).

Vol. 4212: J. Fürnkranz, T. Scheffer, M. Spiliopoulou (Eds.), Machine Learning: ECML 2006. XXIII, 851 pages. 2006. (Sublibrary LNAI).

Vol. 4211: P. Vogt, Y. Sugita, E. Tuci, C. Nehaniv (Eds.), Symbol Grounding and Beyond. VIII, 237 pages. 2006. (Sublibrary LNAI).

Vol. 4209: F. Crestani, P. Ferragina, M. Sanderson (Eds.), String Processing and Information Retrieval. XIV, 367 pages. 2006.

Vol. 4208: M. Gerndt, D. Kranzlmüller (Eds.), High Performance Computing and Communications. XXII, 938 pages. 2006.

Vol. 4207: Z. Ésik (Ed.), Computer Science Logic. XII, 627 pages. 2006.

Vol. 4206: P. Dourish, A. Friday (Eds.), UbiComp 2006: Ubiquitous Computing. XIX, 526 pages. 2006.

Vol. 4205: G. Bourque, N. El-Mabrouk (Eds.), Comparative Genomics. X, 231 pages. 2006. (Sublibrary LNBI).

Vol. 4204: F. Benhamou (Ed.), Principles and Practice of Constraint Programming - CP 2006. XVIII, 774 pages. 2006.

Vol. 4203: F. Esposito, Z.W. Raś, D. Malerba, G. Semeraro (Eds.), Foundations of Intelligent Systems. XVIII, 767 pages. 2006. (Sublibrary LNAI).

Vol. 4202: E. Asarin, P. Bouyer (Eds.), Formal Modeling and Analysis of Timed Systems. XI, 369 pages. 2006.

Vol. 4201: Y. Sakakibara, S. Kobayashi, K. Sato, T. Nishino, E. Tomita (Eds.), Grammatical Inference: Algorithms and Applications. XII, 359 pages. 2006. (Sublibrary LNAI).

Vol. 4199: O. Nierstrasz, J. Whittle, D. Harel, G. Reggio (Eds.), Model Driven Engineering Languages and Systems. XVI, 798 pages. 2006.

Vol. 4197: M. Raubal, H.J. Miller, A.U. Frank, M.F. Goodchild (Eds.), Geographic, Information Science. XIII, 419 pages. 2006.

Vol. 4196: K. Fischer, I.J. Timm, E. André, N. Zhong (Eds.), Multiagent System Technologies. X, 185 pages. 2006. (Sublibrary LNAI).

Vol. 4195: D. Gaiti, G. Pujolle, E. Al-Shaer, K. Calvert, S. Dobson, G. Leduc, O. Martikainen (Eds.), Autonomic Networking. IX, 316 pages. 2006.

Vol. 4194: V.G. Ganzha, E.W. Mayr, E.V. Vorozhtsov (Eds.), Computer Algebra in Scientific Computing. XI, 313 pages. 2006.

Vol. 4193: T.P. Runarsson, H.-G. Beyer, E. Burke, J.J. Merelo-Guervós, L. D. Whitley, X. Yao (Eds.), Parallel Problem Solving from Nature - PPSN IX. XIX, 1061 pages. 2006.

Vol. 4192: B. Mohr, J.L. Träff, J. Worringen, J. Dongarra (Eds.), Recent Advances in Parallel Virtual Machine and Message Passing Interface. XVI, 414 pages. 2006.

Vol. 4191: R. Larsen, M. Nielsen, J. Sporring (Eds.), Medical Image Computing and Computer-Assisted Intervention – MICCAI 2006, Part II. XXXVIII, 981 pages. 2006.

Vol. 4190: R. Larsen, M. Nielsen, J. Sporring (Eds.), Medical Image Computing and Computer-Assisted Intervention – MICCAI 2006, Part I. XXXVVIII, 949 pages. 2006.

Vol. 4189: D. Gollmann, J. Meier, A. Sabelfeld (Eds.), Computer Security – ESORICS 2006. XI, 548 pages. 2006.

Vol. 4188: P. Sojka, I. Kopeček, K. Pala (Eds.), Text, Speech and Dialogue. XIV, 721 pages. 2006. (Sublibrary LNAI).

Vol. 4187: J.J. Alferes, J. Bailey, W. May, U. Schwertel (Eds.), Principles and Practice of Semantic Web Reasoning. XI, 277 pages. 2006.

Vol. 4186: C. Jesshope, C. Egan (Eds.), Advances in Computer Systems Architecture. XIV, 605 pages. 2006.

Vol. 4185: R. Mizoguchi, Z. Shi, F. Giunchiglia (Eds.), The Semantic Web – ASWC 2006. XX, 778 pages. 2006.

Vol. 4184: M. Bravetti, M. Núñez, G. Zavattaro (Eds.), Web Services and Formal Methods. X, 289 pages. 2006.

Vol. 4183: J. Euzenat, J. Domingue (Eds.), Artificial Intelligence: Methodology, Systems, and Applications. XIII, 291 pages. 2006. (Sublibrary LNAI).

Vol. 4182: H.T. Ng, M.-K. Leong, M.-Y. Kan, D. Ji (Eds.), Information Retrieval Technology. XVI, 684 pages. 2006.

Vol. 4180: M. Kohlhase, OMDoc – An Open Markup Format for Mathematical Documents [version 1.2]. XIX, 428 pages. 2006. (Sublibrary LNAI).

Vol. 4179: J. Blanc-Talon, W. Philips, D. Popescu, P. Scheunders (Eds.), Advanced Concepts for Intelligent Vision Systems. XXIV, 1224 pages. 2006.

Vol. 4178: A. Corradini, H. Ehrig, U. Montanari, L. Ribeiro, G. Rozenberg (Eds.), Graph Transformations. XII, 473 pages. 2006.

Vol. 4177: R. Marín, E. Onaindía, A. Bugarín, J. Santos (Eds.), Current Topics in Artificial Intelligence. XIII, 621 pages. 2006. (Sublibrary LNAI).

Vol. 4176: S.K. Katsikas, J. Lopez, M. Backes, S. Gritzalis, B. Preneel (Eds.), Information Security. XIV, 548 pages. 2006.

Vol. 4175: P. Bücher, B.M.E. Moret (Eds.), Algorithms in Bioinformatics. XII, 402 pages. 2006. (Sublibrary LNBI).

Vol. 4174: K. Franke, K.-R. Müller, B. Nickolay, R. Schäfer (Eds.), Pattern Recognition. XX, 773 pages. 2006.

Vol. 4173: S. El Yacoubi, B. Chopard, S. Bandini (Eds.), Cellular Automata. XV, 734 pages. 2006.

Vol. 4172: J. Gonzalo, C. Thanos, M. F. Verdejo, R.C. Carrasco (Eds.), Research and Advanced Technology for Digital Libraries. XVII, 569 pages. 2006.

Vol. 4169: H.L. Bodlaender, M.A. Langston (Eds.), Parameterized and Exact Computation. XI, 279 pages. 2006.

Vol. 4168: Y. Azar, T. Erlebach (Eds.), Algorithms – ESA 2006. XVIII, 843 pages. 2006.

Vol. 4167: S. Dolev (Ed.), Distributed Computing. XV, 576 pages. 2006.

Vol. 4166: J. Górski (Ed.), Computer Safety, Reliability, and Security. XIV, 440 pages. 2006.

Vol. 4165: W. Jonker, M. Petković (Eds.), Secure, Data Management. X, 185 pages. 2006.

Vol. 4163: H. Bersini, J. Carneiro (Eds.), Artificial Immune Systems. XII, 460 pages. 2006.

Vol. 4162: R. Královič, P. Urzyczyn (Eds.), Mathematical Foundations of Computer Science 2006. XV, 814 pages. 2006.

Vol. 4161: R. Harper, M. Rauterberg, M. Combetto (Eds.), Entertainment Computing - ICEC 2006. XXVII, 417 pages. 2006.

Vol. 4160: M. Fisher, W.v.d. Hoek, B. Konev, A. Lisitsa (Eds.), Logics in Artificial Intelligence. XII, 516 pages. 2006. (Sublibrary LNAI).

Vol. 4159: J. Ma, H. Jin, L.T. Yang, J.J.-P. Tsai (Eds.), Ubiquitous Intelligence and Computing. XXII, 1190 pages. 2006.

Vol. 4158: L.T. Yang, H. Jin, J. Ma, T. Ungerer (Eds.), Autonomic and Trusted Computing. XIV, 613 pages. 2006.

Vol. 4156: S. Amer-Yahia, Z. Bellahsène, E. Hunt, R. Unland, J.X. Yu (Eds.), Database and XML Technologies. IX, 123 pages. 2006.

Vol. 4155: O. Stock, M. Schaerf (Eds.), Reasoning, Action and Interaction in AI Theories and Systems. XVIII, 343 pages. 2006. (Sublibrary LNAI).

Vol. 4154: Y.A. Dimitriadis, I. Zigurs, E. Gómez-Sánchez (Eds.), Groupware: Design, Implementation, and Use. XIV, 438 pages. 2006.

Vol. 4153: N. Zheng, X. Jiang, X. Lan (Eds.), Advances in Machine Vision, Image Processing, and Pattern Analysis. XIII, 506 pages. 2006.

Vol. 4152: Y. Manolopoulos, J. Pokorný, T. Sellis (Eds.), Advances in Databases and Information Systems. XV, 448 pages. 2006.

Vol. 4151: A. Iglesias, N. Takayama (Eds.), Mathematical Software - ICMS 2006. XVII, 452 pages. 2006.

Vol. 4150: M. Dorigo, L.M. Gambardella, M. Birattari, A. Martinoli, R. Poli, T. Stützle (Eds.), Ant Colony Optimization and Swarm Intelligence. XVI, 526 pages. 2006.

Vol. 4149: M. Klusch, M. Rovatsos, T.R. Payne (Eds.), Cooperative Information Agents X. XII, 477 pages. 2006. (Sublibrary LNAI).

Vol. 4148: J. Vounckx, N. Azemard, P. Maurine (Eds.), Integrated Circuit and System Design. XVI, 677 pages. 2006.

Vol. 4147: M. Broy, I.H. Krüger, M. Meisinger (Eds.), Automotive Software – Connected Services in Mobile Networks. XIV, 155 pages. 2006.

Vol. 4146: J.C. Rajapakse, L. Wong, R. Acharya (Eds.), Pattern Recognition in Bioinformatics. XIV, 186 pages. 2006. (Sublibrary LNBI).

Vol. 4145: L. Moreau, I. Foster (Eds.), Provenance and Annotation of Data and Processes. XI, 288 pages. 2006.

¥513.00元
此为试读，需要完整PDF请访问：www.ertongbook.com

Table of Contents

Side Channels I

Low Resources

Invited Talk I

Hardware Attacks and Countermeasures I

Special Purpose Hardware

Efficient Algorithms for Embedded Processors

Side Channels II

Invited Talk II

Hardware Attacks and Countermeasures II

Efficient Hardware I

Trusted Computing

Side Channels III

Hardware Attacks and Countermeasures III

Invited Talk III

Efficient Hardware II

Template Attacks in Principal Subspaces

C. Archambeau, E. Peeters, F.-X. Standaert, and J.-J. Quisquater

UCL Crypto Group - Université catholique de Louvain
Place du Levant 3, B-1348 Louvain-la-Neuve, Belgium
{archambeau, peeters, standaert, jjq}@dice.ucl.ac.be

Abstract. Side-channel attacks are a serious threat to implementations of cryptographic algorithms. Secret information is recovered based on power consumption, electromagnetic emanations or any other form of physical information leakage. Template attacks are probabilistic side-channel attacks, which assume a Gaussian noise model. Using the maximum likelihood principle enables us to reveal (part of) the secret for each set of recordings (i.e., leakage trace). In practice, however, the major concerns are (i) how to select the points of interest of the traces, (ii) how to choose the minimal distance between these points, and (iii) how many points of interest are needed for attacking. So far, only heuristics were provided. In this work, we propose to perform template attacks in the principal subspace of the traces. This new type of attack addresses all practical issues in principled way and automatically. The approach is validated by attacking stream ciphers such as RC4. We also report analysis results of template style attacks against an FPGA implementation of AES Rijndael. Roughly, the template attack we carried out requires five time less encrypted messages than the best reported correlation attack against similar block cipher implementations.

1 Introduction

Since their first public appearance in 1996 [6], side-channel attacks have been intensively studied by the cryptographic community. The basic principle is to monitor one (or more) unintentional channels that leak from a device such as a smart card and to match these observations with a key-dependent leakage prediction. This channel is usually monitored thanks to an oscilloscope that samples a continuous analog signal and turns it into a discrete digitalized sequence. This sequence is often referred to as a trace.

Recently, a probabilistic side-channel attack, called the Template Attack (TA), was introduced [2]. This attack was originally mounted to target stream ciphers implementation. In this context, the attacker can only observe a single use of the key, usually during the initialization step of the cipher. As it is not possible to generate different leakages from the same secret key (e.g., corresponding to different plaintexts), TAs were purposed for a more efficient way of retrieving information from side-channel traces.

There are three main reasons that make TAs more efficient than previous approaches to exploit side-channel leakages. First, TAs usually require a profiling step, in order to build a (probabilistic) noise model of the side-channel

L. Goubin and M. Matsui (Eds.): CHES 2006, LNCS 4249, pp. 1–14, 2006.
© International Association for Cryptologic Research 2006

that can be used to capture the secret information leaked by a running device. Second, TAs usually exploit multivariate statistics to characterize the dependencies between the different time instant in the traces. Finally, TAs use maximum likelihood as similarity measure, that can capture any type of dependency (if the probabilistic model is found to be adequate), whereas, for example correlation analysis only captures linear dependencies [1]. In general, the cost of these improvements is a reduction of the adversarial flexibility. For example, Hamming weight leakage models can generally be used for any CMOS devices while template attacks profile the leakage function for one particular device.

TA relies on the hypothesis that leakage information is located in the variability of the leakage traces. In order to recover the secret, one has thus to focus at the time instants where the variability is maximal. However, in practice it is not clear how many and which moments exactly are important. The attacks are therefore based on heuristics, which specify these quantities according to some prior belief. For example, it is common to force the successive, relevant time instants to be one clock cycle distant.

The main contribution of this work is that we take TA a step further. Instead of applying TA directly, we first transform the leakage traces such that we are able to select the relevant features (i.e. transformed time instants) and their number automatically. Meanwhile, we do not need to determine a specific feature interdistance. Of course, when performing TA after transformation, we still take the correlations between the features into account. Now, in order to find a suitable transformation consider again ordinary TA. It is assumed that the secret information leakage is mainly hidden in the local variability of the mean traces. If this hypothesis is valid, it would be more appropriate to take the optimal linear combination of the relevant time samples and perform TA in the principal subspace of the mean traces. We call this approach principal subspace-based TA (PSTA). A principal subspace can be viewed as a lower dimensional subspace embedded in the data space[1] where each coordinate axis successively indicates the direction in which the data have maximal variability (or variance).

A standard statistical tool for finding the principal subspace of a data set is principal component analysis (PCA) [5]. PCA performs an eigendecomposition of the empirical data covariance matrix in order to identify, both, the principal directions (eigenvectors) and the variance (eigenvalues) associated to each one of them. However, practical issues may arise in the context of PSTA, as the dimension of the traces is much larger, (typically $\mathcal{O}(10^5)$) than the number of traces (typically $\mathcal{O}(10^3)$). Therefore, we propose to use a variant of PCA that is more suitable in this situation (see Section 3.1 for further details).

An attractive feature of PSTA is that the projected traces are aligned with the directions of maximal variance. These directions are nothing else than a weighted sum of all the time instants, the weights being determined such that the data variability is preserved after projection. So, in contrast to TA, which selects a relevant subset of time instants according to a heuristic, PSTA determines first the optimal (in terms of maximal variance) linear combination of these time

[1] Here, the data space is the space in which the leakage traces live.

此为试读,需要完整PDF请访问: www.ertongbook.com