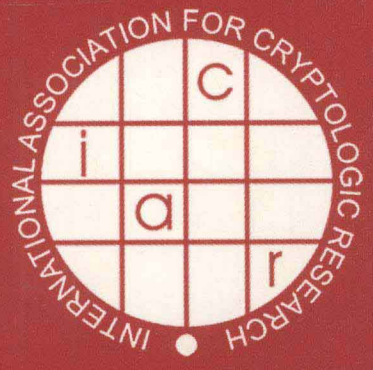
Josyula R. Rao
Berk Sunar (Eds.)

LNCS 3659

Cryptographic Hardware and Embedded Systems – CHES 2005

7th International Workshop
Edinburgh, UK, August/September 2005
Proceedings



Springer

Josyula R. Rao Berk Sunar (Eds.)

Cryptographic Hardware and Embedded Systems – CHES 2005

7th International Workshop
Edinburgh, UK, August 29 – September 1, 2005
Proceedings

Springer

Volume Editors

Josyula R. Rao
IBM T.J. Watson Research Center
19 Skyline Drive, Hawthorne, NY 10532, USA
E-mail: jrrao@us.ibm.com

Berk Sunar
Worcester Polytechnical Institute
Department of Electrical and Computer Engineering
100 Institute Road, Worcester, MA 01609, USA
E-mail: sunar@wpi.edu

Library of Congress Control Number: 2005931119

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

ISSN 0302-9743
ISBN-10 3-540-28474-5 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-28474-1 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 11545262 06/3142 5 4 3 2 1 0

Lecture Notes in Computer Science 3659

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

Editorial Board

Lecture Notes in Computer Science

For information about Vols. 1–3532

please contact your bookseller or Springer

Vol. 3659: J.R. Rao, B. Sunar (Eds.), Cryptographic Hardware and Embedded Systems – CHES 2005. XIV, 458 pages. 2005.

Vol. 3654: S. Jajodia, D. Wijesekera (Eds.), Data and Applications Security XIX. X, 353 pages. 2005.

Vol. 3653: M. Abadi, L.d. Alfaro (Eds.), CONCUR 2005 – Concurrency Theory. XIV, 578 pages. 2005.

Vol. 3649: W.M.P. van der Aalst, B. Benatallah, F. Casati, F. Curbera (Eds.), Business Process Management. XII, 472 pages. 2005.

Vol. 3639: P. Godefroid (Ed.), Model Checking Software. XI, 289 pages. 2005.

Vol. 3638: A. Butz, B. Fisher, A. Krüger, P. Olivier (Eds.), Smart Graphics. XI, 269 pages. 2005.

Vol. 3634: L. Ong (Ed.), Computer Science Logic. XI, 567 pages. 2005.

Vol. 3633: C. Bauzer Medeiros, M. Egenhofer, E. Bertino (Eds.), Advances in Spatial and Temporal Databases. XIII, 433 pages. 2005.

Vol. 3632: R. Nieuwenhuis (Ed.), Automated Deduction – CADE-20. XIII, 459 pages. 2005. (Subseries LNAI).

Vol. 3627: C. Jacob, M.L. Pilat, P.J. Bentley, J. Timmis (Eds.), Artificial Immune Systems. XII, 500 pages. 2005.

Vol. 3626: B. Ganter, G. Stumme, R. Wille (Eds.), Formal Concept Analysis. X, 349 pages. 2005. (Subseries LNAI).

Vol. 3625: S. Kramer, B. Pfahringer (Eds.), Inductive Logic Programming. XIII, 427 pages. 2005. (Subseries LNAI).

Vol. 3624: C. Chekuri, K. Jansen, J.D.P. Rolim, L. Trevisan (Eds.), Approximation, Randomization and Combinatorial Optimization. XI, 495 pages. 2005.

Vol. 3623: M. Liśkiewicz, R. Reischuk (Eds.), Fundamentals of Computation Theory. XV, 576 pages. 2005.

Vol. 3621: V. Shoup (Ed.), Advances in Cryptology – CRYPTO 2005. XI, 568 pages. 2005.

Vol. 3620: H. Muñoz-Avila, F. Ricci (Eds.), Case-Based Reasoning Research and Development. XV, 654 pages. 2005. (Subseries LNAI).

Vol. 3619: X. Lu, W. Zhao (Eds.), Networking and Mobile Computing. XXIV, 1299 pages. 2005.

Vol. 3615: B. Ludäscher, L. Raschid (Eds.), Data Integration in the Life Sciences. XII, 344 pages. 2005. (Subseries LNBI).

Vol. 3614: L. Wang, Y. Jin (Eds.), Fuzzy Systems and Knowledge Discovery, Part II. XLI, 1314 pages. 2005. (Subseries LNAI).

Vol. 3613: L. Wang, Y. Jin (Eds.), Fuzzy Systems and Knowledge Discovery, Part I. XLI, 1334 pages. 2005. (Subseries LNAI).

Vol. 3608: F. Dehne, A. López-Ortiz, J.-R. Sack (Eds.), Algorithms and Data Structures. XIV, 446 pages. 2005.

Vol. 3607: J.-D. Zucker, L. Saitta (Eds.), Abstraction, Reformulation and Approximation. XII, 376 pages. 2005. (Subseries LNAI).

Vol. 3606: V. Malyshkin (Ed.), Parallel Computing Technologies. XII, 470 pages. 2005.

Vol. 3603: J. Hurd, T. Melham (Eds.), Theorem Proving in Higher Order Logics. IX, 409 pages. 2005.

Vol. 3602: R. Eigenmann, Z. Li, S.P. Midkiff (Eds.), Languages and Compilers for High Performance Computing. IX, 486 pages. 2005.

Vol. 3599: U. Aßmann, M. Aksit, A. Rensink (Eds.), Model Driven Architecture. X, 235 pages. 2005.

Vol. 3598: H. Murakami, H. Nakashima, H. Tokuda, M. Yasumura, Ubiquitous Computing Systems. XIII, 275 pages. 2005.

Vol. 3597: S. Shimojo, S. Ichii, T.W. Ling, K.-H. Song (Eds.), Web and Communication Technologies and Internet-Related Social Issues - HSI 2005. XIX, 368 pages. 2005.

Vol. 3596: F. Dau, M.-L. Mugnier, G. Stumme (Eds.), Conceptual Structures: Common Semantics for Sharing Knowledge. XI, 467 pages. 2005. (Subseries LNAI).

Vol. 3595: L. Wang (Ed.), Computing and Combinatorics. XVI, 995 pages. 2005.

Vol. 3594: J.C. Setubal, S. Verjovski-Almeida (Eds.), Advances in Bioinformatics and Computational Biology. XIV, 258 pages. 2005. (Subseries LNBI).

Vol. 3592: S. Katsikas, J. Lopez, G. Pernul (Eds.), Trust, Privacy and Security in Digital Business. XII, 332 pages. 2005.

Vol. 3591: M.A. Wimmer, R. Traunmüller, Å. Grönlund, K.V. Andersen (Eds.), Electronic Government. XIII, 317 pages. 2005.

Vol. 3590: K. Bauknecht, B. Pröll, H. Werthner (Eds.), E-Commerce and Web Technologies. XIV, 380 pages. 2005.

Vol. 3587: P. Perner, A. Imiya (Eds.), Machine Learning and Data Mining in Pattern Recognition. XVII, 695 pages. 2005. (Subseries LNAI).

Vol. 3586: A.P. Black (Ed.), ECOOP 2005 - Object-Oriented Programming. XVII, 631 pages. 2005.

Vol. 3584: X. Li, S. Wang, Z.Y. Dong (Eds.), Advanced Data Mining and Applications. XIX, 835 pages. 2005. (Subseries LNAI).

Vol. 3583: R.W. H. Lau, Q. Li, R. Cheung, W. Liu (Eds.), Advances in Web-Based Learning – ICWL 2005. XIV, 420 pages. 2005.

Vol. 3582: J. Fitzgerald, I.J. Hayes, A. Tarlecki (Eds.), FM 2005: Formal Methods. XIV, 558 pages. 2005.

Vol. 3581: S. Miksch, J. Hunter, E. Keravnou (Eds.), Artificial Intelligence in Medicine. XVII, 547 pages. 2005. (Subseries LNAI).

Vol. 3580: L. Caires, G.F. Italiano, L. Monteiro, C. Palamidessi, M. Yung (Eds.), Automata, Languages and Programming. XXV, 1477 pages. 2005.

Vol. 3579: D. Lowe, M. Gaedke (Eds.), Web Engineering. XXII, 633 pages. 2005.

Vol. 3578: M. Gallagher, J. Hogan, F. Maire (Eds.), Intelligent Data Engineering and Automated Learning - IDEAL 2005. XVI, 599 pages. 2005.

Vol. 3577: R. Falcone, S. Barber, J. Sabater-Mir, M.P. Singh (Eds.), Trusting Agents for Trusting Electronic Societies. VIII, 235 pages. 2005. (Subseries LNAI).

Vol. 3576: K. Etessami, S.K. Rajamani (Eds.), Computer Aided Verification. XV, 564 pages. 2005.

Vol. 3575: S. Wermter, G. Palm, M. Elshaw (Eds.), Biomimetic Neural Learning for Intelligent Robots. IX, 383 pages. 2005. (Subseries LNAI).

Vol. 3574: C. Boyd, J.M. González Nieto (Eds.), Information Security and Privacy. XIII, 586 pages. 2005.

Vol. 3573: S. Etalle (Ed.), Logic Based Program Synthesis and Transformation. VIII, 279 pages. 2005.

Vol. 3572: C. De Felice, A. Restivo (Eds.), Developments in Language Theory. XI, 409 pages. 2005.

Vol. 3571: L. Godo (Ed.), Symbolic and Quantitative Approaches to Reasoning with Uncertainty. XVI, 1028 pages. 2005. (Subseries LNAI).

Vol. 3570: A. S. Patrick, M. Yung (Eds.), Financial Cryptography and Data Security. XII, 376 pages. 2005.

Vol. 3569: F. Bacchus, T. Walsh (Eds.), Theory and Applications of Satisfiability Testing. XII, 492 pages. 2005.

Vol. 3568: W.-K. Leow, M.S. Lew, T.-S. Chua, W.-Y. Ma, L. Chaisorn, E.M. Bakker (Eds.), Image and Video Retrieval. XVII, 672 pages. 2005.

Vol. 3567: M. Jackson, D. Nelson, S. Stirk (Eds.), Database: Enterprise, Skills and Innovation. XII, 185 pages. 2005.

Vol. 3566: J.-P. Banâtre, P. Fradet, J.-L. Giavitto, O. Michel (Eds.), Unconventional Programming Paradigms. XI, 367 pages. 2005.

Vol. 3565: G.E. Christensen, M. Sonka (Eds.), Information Processing in Medical Imaging. XXI, 777 pages. 2005.

Vol. 3564: N. Eisinger, J. Małuszyński (Eds.), Reasoning Web. IX, 319 pages. 2005.

Vol. 3562: J. Mira, J.R. Álvarez (Eds.), Artificial Intelligence and Knowledge Engineering Applications: A Bioinspired Approach, Part II. XXIV, 636 pages. 2005.

Vol. 3561: J. Mira, J.R. Álvarez (Eds.), Mechanisms, Symbols, and Models Underlying Cognition, Part I. XXIV, 532 pages. 2005.

Vol. 3560: V.K. Prasanna, S. Iyengar, P.G. Spirakis, M. Welsh (Eds.), Distributed Computing in Sensor Systems. XV, 423 pages. 2005.

Vol. 3559: P. Auer, R. Meir (Eds.), Learning Theory. XI, 692 pages. 2005. (Subseries LNAI).

Vol. 3558: V. Torra, Y. Narukawa, S. Miyamoto (Eds.), Modeling Decisions for Artificial Intelligence. XII, 470 pages. 2005. (Subseries LNAI).

Vol. 3557: H. Gilbert, H. Handschuh (Eds.), Fast Software Encryption. XI, 443 pages. 2005.

Vol. 3556: H. Baumeister, M. Marchesi, M. Holcombe (Eds.), Extreme Programming and Agile Processes in Software Engineering. XIV, 332 pages. 2005.

Vol. 3555: T. Vardanega, A.J. Wellings (Eds.), Reliable Software Technology – Ada-Europe 2005. XV, 273 pages. 2005.

Vol. 3554: A. Dey, B. Kokinov, D. Leake, R. Turner (Eds.), Modeling and Using Context. XIV, 572 pages. 2005. (Subseries LNAI).

Vol. 3553: T.D. Hämäläinen, A.D. Pimentel, J. Takala, S. Vassiliadis (Eds.), Embedded Computer Systems: Architectures, Modeling, and Simulation. XV, 476 pages. 2005.

Vol. 3552: H. de Meer, N. Bhatti (Eds.), Quality of Service – IWQoS 2005. XVIII, 400 pages. 2005.

Vol. 3551: T. Härder, W. Lehner (Eds.), Data Management in a Connected World. XIX, 371 pages. 2005.

Vol. 3548: K. Julisch, C. Kruegel (Eds.), Intrusion and Malware Detection and Vulnerability Assessment. X, 241 pages. 2005.

Vol. 3547: F. Bomarius, S. Komi-Sirviö (Eds.), Product Focused Software Process Improvement. XIII, 588 pages. 2005.

Vol. 3546: T. Kanade, A. Jain, N.K. Ratha (Eds.), Audio- and Video-Based Biometric Person Authentication. XX, 1134 pages. 2005.

Vol. 3544: T. Higashino (Ed.), Principles of Distributed Systems. XII, 460 pages. 2005.

Vol. 3543: L. Kutvonen, N. Alonistioti (Eds.), Distributed Applications and Interoperable Systems. XI, 235 pages. 2005.

Vol. 3542: H.H. Hoos, D.G. Mitchell (Eds.), Theory and Applications of Satisfiability Testing. XIII, 393 pages. 2005.

Vol. 3541: N.C. Oza, R. Polikar, J. Kittler, F. Roli (Eds.), Multiple Classifier Systems. XII, 430 pages. 2005.

Vol. 3540: H. Kalviainen, J. Parkkinen, A. Kaarna (Eds.), Image Analysis. XXII, 1270 pages. 2005.

Vol. 3539: K. Morik, J.-F. Boulicaut, A. Siebes (Eds.), Local Pattern Detection. XI, 233 pages. 2005. (Subseries LNAI).

Vol. 3538: L. Ardissono, P. Brna, A. Mitrovic (Eds.), User Modeling 2005. XVI, 533 pages. 2005. (Subseries LNAI).

Vol. 3537: A. Apostolico, M. Crochemore, K. Park (Eds.), Combinatorial Pattern Matching. XI, 444 pages. 2005.

Vol. 3536: G. Ciardo, P. Darondeau (Eds.), Applications and Theory of Petri Nets 2005. XI, 470 pages. 2005.

Vol. 3535: M. Steffen, G. Zavattaro (Eds.), Formal Methods for Open Object-Based Distributed Systems. X, 323 pages. 2005.

Vol. 3534: S. Spaccapietra, E. Zimányi (Eds.), Journal on Data Semantics III. XI, 213 pages. 2005.

Vol. 3533: M. Ali, F. Esposito (Eds.), Innovations in Applied Artificial Intelligence. XX, 858 pages. 2005. (Subseries LNAI).

Preface

These are the proceedings of the 7th Workshop on Cryptographic Hardware and Embedded Systems (CHES 2005) held in Edinburgh, Scotland from August 29 to September 1, 2005. The CHES workshop has been sponsored by the International Association for Cryptologic Research (IACR) for the last two years.

We received a total of 108 paper submissions for CHES 2005. The double-blind review process involved a 27-member program committee and a large number of external sub-referees. The review process concluded with a two week discussion process which resulted in 32 papers being selected for presentation. We are grateful to the program committee members and the external sub-referees for carrying out such an enormous task. Unfortunately, there were many strong papers that could not be included in the program due to a lack of space. We would like to thank all our colleagues who submitted papers to CHES 2005.

In addition to regular presentations, there were three excellent invited talks given by Ross Anderson (University of Cambridge) on "What Identity Systems Can and Cannot Do", by Thomas Wille (Philips Semiconductors Inc) on "Security of Identification Products: How to Manage", and by Jim Ward (Trusted Computing Group and IBM) on "Trusted Computing in Embedded Systems". It also included a rump session, chaired by Christof Paar, featuring informal talks on recent results.

The focus of CHES 2005 was similar to that of the earlier CHES workshops with the addition of a few new topics of emerging interest among which were smart card attacks and architectures, tamper resistance on the chip and board level, true and pseudo random number generators, special-purpose hardware for cryptanalysis, embedded security, cryptography for pervasive computing (e.g., RFID, sensor networks), device identification, non-classical cryptographic technologies, and side channel cryptanalysis. Special attention was paid to trusted computing platforms.

Special compliments go out to Colin D. Walter, the general chair and local organizer of CHES 2005, who brought the workshop to the beautiful historic town of Edinburgh, Scotland making it as much of a cultural event as a stimulating technical gathering. Christof Paar held the publicity Chair of CHES and was helpful at all stages of the organization. We would like to thank our corporate sponsors Cryptography Research Inc., escrypt GmbH, Gemplus, IBM, and RSA Security, who made it possible to have a lively event with their generous contributions. We would like to thank our dedicated webmaster Jens-Peter Kaps for maintaining the CHES website and review system even when he was travelling. Finally, we would like to thank the CHES steering committee members for giving us the honor of being part of such an influential conference.

August 2005 Josyula R. Rao and Berk Sunar

7th Workshop on Cryptographic Hardware and Embedded Systems

August 29 – September 1, 2005, Edinburgh, Scotland
http://www.chesworkshop.org/

Organizing Committee

Colin D. Walter (General Chair) ..... Comodo Research Lab, UK
Christof Paar (Publicity Chair) ..... Ruhr-Universität Bochum, Germany
Josyula R. Rao (Program Co-chair) .. IBM T.J. Watson Research Center, USA
Berk Sunar (Program Co-chair) ..... Worcester Polytechnic Institute, USA

Program Committee

Ross Anderson ..... Cambridge University, UK
Mohammed Benaissa ..... The University of Sheffield, UK
Suresh Chari ..... IBM T.J. Watson Research Center, USA
Kris Gaj ..... George Mason University, USA
Louis Goubin ..... Université de Versailles-St-Quentin-en-Yvelines, France
Jorge Guajardo ..... Infineon Technologies, Germany
Çetin Kaya Koç ..... Oregon State University, USA
Peter Kornerup ..... University of Southern Denmark, Denmark
Pil Joong Lee ..... Postech, South Korea
David Naccache ..... Gemplus, France and
Royal Holloway, University of London, UK
Elisabeth Oswald ..... Graz University of Technology, Austria
Christof Paar ..... Ruhr-Universität Bochum, Germany
Daniel Page ..... University of Bristol, UK
Bart Preneel ..... Katholieke Universiteit Leuven, Belgium
Pankaj Rohatgi ..... IBM T.J. Watson Research Center, USA
Ahmad Sadeghi ..... Ruhr-University Bochum, Germany
Kouichi Sakurai ..... Kyushu University, Japan
David Samyde ..... FemtoNano, France
Erkay Savaş ..... Sabanci University, Turkey
Werner Schindler ..... Bundesamt für Sicherheit
in der Informationstechnik, Germany
Jean-Pierre Seifert ..... Intel, USA
Nigel Smart ..... University of Bristol, UK
Francois-Xavier Standaert ..... Université Catholique de Louvain, Belgium

Tsuyoshi Takagi ..... Future University, Hakodate, Japan
Elena Trichina ..... Spansion, USA
Ingrid Verbauwhede .. ESAT/COSIC Division, Katholieke Universiteit, Leuven
Colin Walter ..... Comodo Research Lab, UK

Steering Committee

Marc Joye ..... Gemplus, Card Security Group, France
Burt Kaliski ..... RSA Laboratories, USA
Çetin Kaya Koç ..... Oregon State University, USA
Christof Paar ..... Ruhr-Universität Bochum, Germany
Jean-Jacques Quisquater ..... Université Catholique de Louvain, Belguim
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
Dakshi Agrawal
Mehdi-Laurent Akkar
Roberto Avanzi
Murat Aydos
Yoo Jin Baek
Lelia Barlow
Lejla Batina
Chevallier-Mames Benoit
Guido Bertoni
Régis Bevan
Mike Bond
Eric Brier
Julien Brouchier
Christophe De Cannière
Dario Carluccio
Laurent Caussou
Juyoung Cha
Herve Chabanne
Nam Su Chang
Kookrae Cho
Mathieu Ciet
Jolyon Clulow
Jean-Sbastien Coron
Nicolas Courtois
Colin van Dyke
Serdar S. Erdem
Martin Feldhofer
Patrick Felke
Wieland Fischer
Jacques J.A. Fournier
Patrick George
Christophe Giraud
Robert Granger
Johann Großschädl
Adnan Gutub
Ghaith Hammouri
Dong Guk Han
Helena Handschuh
Oliver Hauck
Alireza Hodjat
Tetsuya Izu
Mark Jung
Charanjit Jutla
Deniz Karakoyunlu
Paul Karger
Manabu Katagi
Alisher Anatolyevich Kholmatov
Tae Hyun Kim
Minho Kim
Shinsaku Kiyomoto
François Koeune
Sandeep Kumar
Klaus Kursawe
Soonhak Kwon
Gerard Lai
Joe Lano
Peter Leadbitter
Hyang-Sook Lee
Jung Wook Lee
Kerstin Lemke
HuiYun Li
Marco Macchetti
François Macé
Stefan Mangard
Marian Margraf
Nele Mentens
Atsuko Miyaji
Christophe Mourtel
Elke de Mulder
Robert Mullins

Michael Neve
Richard Noad
Francis Olivier
Gerardo Orlando
Siddika Berna Ors
Pascal Paillier
Fabrice Pautot
Matthew Parker
Eric Peeters
Jan Pelzl
Gilles Piret
Thomas Popp
Axel Poschmann
Christine Priplata
Kumar Ranganathan
Nalini Ratha
Arash Reyhani-Masoleh
Gaël Rouvroy
Andy Rupp
Reiner Sailer
Junichiro Saito
Ryuichi Sakai
Yasuyuki Sakai
Kazuo Sakiyama
Gökay Saldamlı
Hisayoshi Sato
Akashi Satoh
Daniel Schepers
Jörg Schwenk
Kai Schramm
Jong Hoon Shin
Jamshid Shokrollahi
Nicolas Sklavos
Sergei Skorobogatov
Colin Stahlke
Martijn Stam
Makoto Sugita
Katsuyuki Takashima
Stefan Tillich
Michael Tunstall
Shigenori Uchuyama
Guy Vandenbosch
Ihor Vasylstov
Frederik Vercauteren
Karine Villegas
Camille Vuillaume
Andre Weimerskirch
Claire Whelan
Christopher Wolf
Johannes Wolkerstorfer
Thomas Wollinger
Yeon Hyeong Yang
Jeong Il Yoon
Young Tae Youn

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-Verlag, 1999.

CHES 2000: Çetin K. Koç and Christof Paar (Editors). *Cryptographic Hardware and Embedded Systems – CHES 2000*, vol. 1965 of *Lecture Notes in Computer Science*, Springer-Verlag, 2000.

CHES 2001: Çetin K. Koç, David Naccache, and Christof Paar (Editors). *Cryptographic Hardware and Embedded Systems – CHES 2001*, vol. 2162 of *Lecture Notes in Computer Science*, Springer-Verlag, 2001.

CHES 2002: Burton S. Kaliski, Çetin K. Koç, and Christof Paar (Editors). *Cryptographic Hardware and Embedded Systems – CHES 2002*, vol. 2523 of *Lecture Notes in Computer Science*, Springer-Verlag, 2002.

CHES 2003: Colin D. Walter, Çetin K. Koç, and Christof Paar (Editors). *Cryptographic Hardware and Embedded Systems – CHES 2003*, vol. 2779 of *Lecture Notes in Computer Science*, Springer-Verlag, 2003.

CHES 2004: Marc Joye and Jean-Jacques Quisquater (Editors). *Cryptographic Hardware and Embedded Systems – CHES 2004*, vol. 3156 of *Lecture Notes in Computer Science*, Springer-Verlag, 2004.

Table of Contents

Hardware Attacks and Countermeasures I

Arithmetic for Cryptography

Side Channel II (EM)

Side Channel III

Trusted Computing

Hardware Attacks and Countermeasures II

Hardware Attacks and Countermeasures III

Efficient Hardware I

Efficient Hardware II

Resistance of Randomized Projective Coordinates Against Power Analysis

William Dupuy and Sébastien Kunz-Jacques

DCSSI Crypto Lab,
51, bd de Latour-Maubourg, 75700 PARIS 07 SP
william.dupuy@laposte.net
kunzjacq@yahoo.fr

Abstract. Embedded devices implementing cryptographic services are the result of a trade-off between cost, performance and security. Aside from flaws in the protocols and the algorithms used, one of the most serious threats against secret data stored in such devices is Side Channel Analysis.

Implementing Public Key Cryptography in low-profile devices such as smart cards is particularly challenging given the computational complexity of the operations involved. In the area of elliptic curve cryptography, some choices of curves and coefficient fields are known to speed up computations, like scalar multiplication. From a theoretical standpoint, the use of optimized structures does not seem to weaken the cryptosystems which use them. Therefore several standardization bodies, such as the NIST, recommend such choices of parameters. However, the study of their impact on practical security of implementations may have been underestimated.

In this paper, we present a new chosen-ciphertext Side-Channel Attack on scalar multiplication that applies when optimized parameters, like NIST curves, are used together with some classical anti-SPA and anti-DPA techniques. For a typical exponent size, the attack allows to recover a secret exponent by performing only a few hundred adaptive power measurements.

1 Introduction

The use of elliptic curves for cryptographic purposes was proposed by Miller [10] in 1985 and Koblitz [8] in 1987. Since then, it became an essential part of public key cryptography. In particular, many cryptosystems rely on the intractability of the discrete logarithm problem (DLP) on elliptic curves. The main advantage of this problem is that it is believed to be harder to solve than other number-theoretic problems. As a consequence, for a similar security level, it is possible to use smaller objects than with integer factorization for example. This property is especially attractive for embedded systems, where storage requirements and computation times are critical.

J.R. Rao and B. Sunar (Eds.): CHES 2005, LNCS 3659, pp. 1–14, 2005.

Cryptosystems relying on DLP on elliptic curves use the *scalar multiplication* operation in some large elliptic curve group $(G, +)$

$$P \in G \rightarrow kP \tag{1}$$

where k is a secret data. Because of DLP hardness, it is believed to be infeasible to compute k from the knowledge of one or several pairs (P, kP).

In a situation where no reasonable attack on a cryptographic algorithm is known, Kocher first observed in 1996 [9] that the measurement of the algorithm computation time could still reveal secret information. This paved the way to Side Channel Attacks that take advantage of the measurement of physical signals emitted by a cryptographic device during a computation to gain access to secret data.

Since then, several examples of Side Channel Attacks led to various countermeasures being developed. Concerning scalar multiplication in EC groups, the use of scalar multiplication algorithms with a regular computation flow like *double-and-add always* or *Montgomery Ladder* is an answer to Simple Power Analysis (SPA), while randomized projective coordinates, first proposed by [4], are used to counter Differential Power Analysis (DPA).

In this paper, we present a new side-channel attack against scalar multiplication implementing these countermeasures, when the EC group used is chosen among the NIST [12], ANSI [1] or SEC [13] recommended curves. It is a Goubin-style attack [6] that uses distinguished points whose presence can be detected along the computation by an observation of power traces despite the randomization countermeasure. It leverages the particular shape of the underlying coefficient fields.

The paper is organized as follows. We first briefly review some facts about elliptic curves in section 2. Then section 3 presents some classical Side Channel Attacks and common countermeasures to prevent them. Finally, sections 4 and 5 present the details of our attack.

2 Elliptic Curves

2.1 Elliptic Curve Equation

Let $\mathbb{K}$ be a finite field of characteristic p. Over this field, we set the equation (E)

$$y^2 + a_1xy = x^3 + a_2x^2 + a_4x + a_6$$

The elliptic curve (C) associated to (E) is the set of all points of $\mathbb{K}^2$ satisfying (E), together with a particular point $\mathcal{O}$ called *point at infinity*. $\mathbb{K}$ is the *coefficient field* of the curve.

Up to an affine change of variables, if $p = 2$, we can set $a_1 = 1$ and $a_4 = 0$. The equation can then be rewritten $y^2 + xy = x^3 + a_2x^2 + a_6$. If $p \geq 3$, we can set $a_1 = a_2 = 0$ and then (E) becomes $y^2 = x^3 + a_4x + a_6$.

Together with an addition law, this set forms a commutative group. We do not describe the group law here since it does not play any role in the attack we present.

2.2 Affine and Projective Representation

A point on a curve of equation (E) is a solution of (E). Therefore the simplest representation of a point on a curve of equation (E) is the corresponding solution of (E) in $\mathbb{K}^2$. This is the *affine* representation.

Nevertheless, other representations can be preferred. We are mainly interested in *projective coordinates*. Given $P = (x, y)$ in affine coordinates, its representation in projective coordinates is $P = (xZ, yZ, Z)$ for any $Z \in \mathbb{K}^*$. If a finite solution of (E) is represented by (α, β, γ), then $\gamma \neq 0$. The point at infinity $\mathcal{O}$ is represented by $(0, \beta, 0)$ for any $\beta \neq 0$.

The projective representation is not unique. In fact, for some finite solution (x, y) of (E) with $x \neq 0$ and $y \neq 0$, any of the three projective coordinates can take an arbitrary value in $\mathbb{K}^*$. This observation is the basis of the randomized projective coordinates countermeasure, which we will describe in section 3.2. Projective representation is also used to increase the efficiency of point addition computations since for example, it allows to compute the group law without having to perform modular inversion in the coefficient field.

2.3 Recommended Coefficient Fields for NIST Elliptic Curves

Curves recommended by standardization bodies such as NIST, ANSI, or SEC are usually defined over $\mathbb{F}_p$, or $\mathbb{F}_2[x]/(P)$ where P a primitive polynomial. We focus on NIST recommended curves from now on. Other standardized curves present similar properties as the ones of the NIST.

Curves Defined on Binary Fields. The coefficient field is here of the form $\mathbb{F}_2[x]/(P)$. The primitive polynomials standardized by the NIST are:

$$P_{233}(x) = x^{233} + x^{74} + 1$$
$$P_{283}(x) = x^{283} + x^{12} + x^7 + x^5 + 1$$
$$P_{409}(x) = x^{409} + x^{87} + 1$$
$$P_{571}(x) = x^{571} + x^{10} + x^5 + x^2 + 1$$

We can notice that these polynomials are very sparse. This has to do with hardware efficiency.

Curves Defined on Prime Order Fields. For these curves, the coefficient field is $\mathbb{F}_p$, with p among

$$p_{192} = 2^{192} - 2^{64} - 1$$
$$p_{224} = 2^{224} - 2^{96} + 1$$
$$p_{256} = 2^{256} - 2^{224} + 2^{192} + 2^{96} - 1$$
$$p_{384} = 2^{384} - 2^{128} - 2^{96} + 2^{32} - 1$$
$$p_{521} = 2^{521} - 1$$

As in the binary case, the sparse form of these primes simplifies and speeds up operations in the coefficient field.