Pascal Paillier
Ingrid Verbauwhede (Eds.)

LNCS 4727

Cryptographic Hardware and Embedded Systems – CHES 2007

9th International Workshop
Vienna, Austria, September 2007
Proceedings

Springer

Pascal Paillier Ingrid Verbauwhede (Eds.)

Cryptographic Hardware and Embedded Systems - CHES 2007

9th International Workshop, Vienna, Austria
September 10-13, 2007
Proceedings

Springer

Volume Editors

Pascal Paillier
37 cours de vincennes
75020 Paris, France
E-mail: pascal.pailler@gemalto.com

Ingrid Verbauwhede
Katholieke Universiteit Leuven, ESAT/COSIC
Kasteelpark Arenberg 10
B-3001 Leuven, Belgium
E-mail: iverbauw@esat.kuleuven.be

Library of Congress Control Number: 2007933579

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 3-540-74734-6 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-74734-5 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12118106 06/3180 5 4 3 2 1 0

Lecture Notes in Computer Science 4727

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

Preface

CHES 2007, the ninth workshop on Cryptographic Hardware and Embedded Systems, was sponsored by the International Association for Cryptologic Research (IACR) and held in Vienna, Austria, September 10–13, 2007. The workshop received 99 submissions from 24 countries, of which the Program Committee (39 members from 15 countries) selected 31 for presentation. For the first time in the history of CHES, each submission was reviewed by at least four reviewers instead of three (and at least five for submissions by PC members, those now being limited to two per member) and many submitted papers have received plenty of extra reviews (some papers received up to nine reviews), thus totalling the unprecedented record of 483 reviews overall.

The papers collected in this volume represent cutting-edge worldwide research in the rapidly evolving fields of crypto-hardware, fault-based and side-channel cryptanalysis, and embedded cryptography, at the crossing of academic and industrial research. The wide diversity of subjects appearing in these proceedings covers virtually all related areas and shows our efforts to extend the scope of CHES more than usual. Although a relatively young workshop, CHES is now firmly established as a scientific event of reference appreciated by more and more renowned experts of theory and practice: many high-quality works were submitted, all of which, sadly, could not be accepted. Selecting from so many good works is no easy task and our deepest thanks go to the members of the Program Committee for their involvement, excellence, and team spirit. We are grateful to the numerous external reviewers listed below for their expertise and assistance in our deliberations.

In addition to the contributions appearing in these proceedings, the workshop program included two invited lectures given by Kim Nguyen and Pankaj Rohatgi. The program also included the traditional rump session, chaired by Nigel Smart, featuring short informal talks on late-breaking research news. This year's rump session was augmented with a parallel demo and poster session welcoming informal presentations of prototypes, attack demos and research works. The Program and Steering Committees commonly agreed on giving the CHES 2007 Best Paper Award to two papers: "Arithmetic Operators for Pairing-Based Cryptography" by Jean-Luc Beuchat, Nicolas Brisebarre, Jérémie Detrey and Eiji Okamoto (University of Tsukuba, Université Monnet and École Normale Supérieure de Lyon) and "Side Channel Cryptanalysis of a Higher Order Masking" by Jean-Sébastien Coron, Emmanuel Prouff and Matthieu Rivain (University of Luxembourg and Oberthur Card Systems). The purpose of the award is to formally acknowledge authors of outstanding papers and to recognize excellence in their research works. Interestingly, these two works represent well the two sides of our field: efficient implementations and hardware-based cryptanalysis.

Ingrid and myself deeply thank Elisabeth Oswald (University of Bristol, UK, and Graz University of Technology, Austria), the General Chair of CHES 2007, for her excellent work managing the local organization and orchestrating the conference logistics. We are grateful to Thomas Herlea (KUL, Belgium) for diligently maintaining the Web system. The review and discussion process was run using e-mail and the WebReview software by Wim Moreau and Joris Claessens. We also owe our gratitude to Lejla Batina (also from KUL) for her help in preparing the call for papers and the proceedings. We would like to deeply thank the Steering Committee and personally Jean-Jacques Quisquater (UCL, Belgium) for his support, trust and kind advice at many occasions. We would also like to thank the Institute for Applied Information Processing and Communications (IAIK) of Graz University of Technology for assisting with local arrangements. Our gratitude also goes to our generous sponsors, namely, Cryptography Research, Comodo, Novacard, Thomson, Infineon and IBM. We heartily thank all those who have contributed to make this workshop a reality: we are forever in your debt.

Finally, we would like to profoundly thank and salute all those who, from all over the world, submitted their work to this workshop as well as all the speakers who provided the scientific contents of CHES 2007: the success of the CHES series is their success and reflects every year the vitality of our community.

July 2007

Pascal Paillier
Ingrid Verbauwhede

Organization

Organizational Committee

Program Co-chairs	Pascal Paillier (Gemalto, France) Ingrid Verbauwhede (KUL, Belgium)
General Chair	Elisabeth Oswald (University of Bristol, UK) and Graz University of Technology, Austria
Publicity Chair	Çetin Kaya Koç (Oregon State University, USA)

Program Committee

Lejla Batina	Katholieke Universiteit Leuven, Belgium
Guido Bertoni	STMicroelectronics, Italy
Christophe Clavier	Gemalto, France
Jean-Sébastien Coron	University of Luxembourg, Luxembourg
Joan Daemen	STMicroelectronics, Belgium
Ricardo Dahab	Universidade Estadual de Campinas, Brazil
Pierre-Alain Fouque	ENS, France
Kris Gaj	George Mason University, USA
Henri Gilbert	Orange Labs, France
Jim Goodman	ATI Technologies, Canada
Louis Goubin	Université de Versailles, France
Louis Granboulan	EADS, France
Helena Handschuh	Spansion, France
Tetsuya Izu	Fujitsu Laboratories Ltd, Japan
Marc Joye	Thomson R&D, France
Çetin Kaya Koç	Oregon State University, USA
Markus Kuhn	University of Cambridge, UK
Pil Joong Lee	Postech, South Korea
Stefan Mangard	Infineon Technologies, Germany
Tsutomu Matsumoto	Yokohama National University, Japan
David Naccache	ENS, France
Christof Paar	Ruhr-Universität Bochum, Germany
Anand Ragunathan	NEC labs, USA
Josyula R. Rao	IBM T.J. Watson Research Center, USA
Pankaj Rohatgi	IBM T.J. Watson Research Center, USA
Ahmad-Reza Sadeghi	Ruhr-Universität Bochum, Germany
Akashi Satoh	IBM, Japan
Erkay Savas	Sabanci University, Turkey
Patrick Schaumont	Virginia Tech, USA

Kai Schramm	Renesas, UK
Jean-Pierre Seifert	University of Innsbruck, Austria
Berk Sunar	Worcester Polytechnic Institute, USA
Tsuyoshi Takagi	Future University Hakodate, Japan
Alexander Taubin	Boston University, USA
Pim Tuyls	Philips Research, Netherlands
Kris Tiri	Intel, USA
Frédéric Valette	DGA/CELAR, France
Serge Vaudenay	EPFL, Switzerland
Colin Walter	Comodo CA, UK

External Referees

Onur Acıiçmez	Sergiu Ghetie	Filippo Melzani
Dakshi Agrawal	Benedikt Gierlichs	Bodo Möller
Toru Akishita	Damien Giry	José R. M. Monteiro
Didier Alquié	Gary Graunke	Shiho Moriai
Frédéric Amiel	Johann Groszschaedl	Christophe Mourtel
Diego Aranha	Jorge Guajardo	Seiji Munetoh
Guido Araujo	Tamer Gudu	Toshiya Nakajima
Gildas Avoine	Sylvain Guilley	Michael Neve
Thomas Baignères	Tim Güneysu	Katsuyuki Okeya
Selcuk Baktir	DongGuk Han	Francis Olivier
Johann Barbier	Naofumi Homma	Berna Örs
Paulo S. L. M. Barreto	Kouichi Itoh	Dag Arne Osvik
Come Berbain	Jens-Peter Kaps	Renaud Pacalet
Jean-Luc Beuchat	Mohamed Karroumi	Dan Page
Olivier Billet	Timo Kasper	Sylvain Pasini
Alex Biryukov	Stefan Katzenbeisser	Thomas B. Pedersen
Andrey Bogdanov	Jin Ho Kim	Eric Peeters
Arnaud Boscher	Tae Hyun Kim	Gerardo Pelosi
Luca Breveglieri	Young Mok Kim	Jan Pelzl
Rafael Dantas de Castro	Giray Komurcu	Thomas Peyrin
Benoit Chevallier-Mames	Urlich Kuehn	Raphael C.-W. Phan
Christophe De Cannière	Konrad Kulikowski	Gilles Piret
Marco De Fazio	Sandeep Kumar	Thomas Popp
Hüseyin Demirci	Noboru Kunihiro	Denis Real
Augusto Jun Devegili	Eun Jeong Kwon	Francesco Regazzoni
Alain Durand	Tanja Lange	Jean-Rene Reinhard
Thomas Eisenbarth	Eunjeong Lee	Matthew Robshaw
M. Tolga Eren	Kerstin Lemke-Rust	F. Rodríguez-Henríquez
Benoît Feix	Gaetan Leurent	Andy Rupp
Martin Feldhofer	Albert Levi	Yasuyuki Sakai
Wieland Fischer	J. C. López-Hernández	Kazuo Sakiyama
Berndt M. Gammel	Theo Markettos	Werner Schindler

Michael Scott
Jae Woo Seo
Yannick Seurin
Jong Hoon Shin
Masaaki Shirase
Jamshid Shokrollahi
Eric Simpson
Daisuke Suzuki
Boris Škorić
Masahiko Takenaka
Laurent Théry
Stefan Tillich
Elena Trichina
Michael Tunstall
Gilles Van Assche
Ihor Vasyltsov
Fré Vercauteren
David Vigilant
Martin Vuagnoux
Camille Vuillaume
Marcel Winandy
Johannes Wolkerstorfer
Paul Wooderson
Yeon-Hyeong Yang
Sebastien Zimmer
Xinwen Zhang

Lecture Notes in Computer Science

For information about Vols. 1–4583

please contact your bookseller or Springer

Vol. 4742: I. Stojmenovic, R.K. Thulasiram, L.T. Yang, W. Jia, M. Guo, R.F. de Mello (Eds.), Parallel and Distributed Processing and Applications. XVIII, 308 pages. 2007.

Vol. 4727: P. Paillier, I. Verbauwhede (Eds.), Cryptographic Hardware and Embedded Systems - CHES 2007. XIV, 468 pages. 2007.

Vol. 4720: B. Konev, F. Wolter (Eds.), Frontiers of Combining Systems. X, 2283 pages. 2007. (Sublibrary LNAI).

Vol. 4708: L. Kučera, A. Kučera (Eds.), Mathematical Foundations of Computer Science 2007. XVIII, 764 pages. 2007.

Vol. 4707: O. Gervasi, M.L. Gavrilova (Eds.), Computational Science and Its Applications – ICCSA 2007, Part III. XXIV, 1205 pages. 2007.

Vol. 4706: O. Gervasi, M.L. Gavrilova (Eds.), Computational Science and Its Applications – ICCSA 2007, Part II. XXIII, 1129 pages. 2007.

Vol. 4705: O. Gervasi, M.L. Gavrilova (Eds.), Computational Science and Its Applications – ICCSA 2007, Part I. XLIV, 1169 pages. 2007.

Vol. 4703: L. Caires, V.T. Vasconcelos (Eds.), CONCUR 2007 – Concurrency Theory. XIII, 507 pages. 2007.

Vol. 4697: L. Choi, Y. Paek, S. Cho (Eds.), Advances in Computer Systems Architecture. XIII, 400 pages. 2007.

Vol. 4685: D.J. Veit, J. Altmann (Eds.), Grid Economics and Business Models. XII, 201 pages. 2007.

Vol. 4684: L. Kang, Y. Liu, S. Zeng (Eds.), Evolvable Systems: From Biology to Hardware. XIV, 446 pages. 2007.

Vol. 4683: L. Kang, Y. Liu, S. Zeng (Eds.), Intelligence Computation and Applications. XVII, 663 pages. 2007.

Vol. 4682: D.-S. Huang, L. Heutte, M. Loog (Eds.), Advanced Intelligent Computing Theories and Applications. XXVII, 1373 pages. 2007. (Sublibrary LNAI).

Vol. 4681: D.-S. Huang, L. Heutte, M. Loog (Eds.), Advanced Intelligent Computing Theories and Applications. XXVI, 1379 pages. 2007.

Vol. 4679: A.L. Yuille, S.-C. Zhu, D. Cremers, Y. Wang (Eds.), Energy Minimization Methods in Computer Vision and Pattern Recognition. XII, 494 pages. 2007.

Vol. 4678: J. Blanc-Talon, W. Philips, D. Popescu, P. Scheunders (Eds.), Advanced Concepts for Intelligent Vision Systems. XXIII, 1100 pages. 2007.

Vol. 4673: W.G. Kropatsch, M. Kampel, A. Hanbury (Eds.), Computer Analysis of Images and Patterns. XX, 1006 pages. 2007.

Vol. 4671: V. Malyshkin (Ed.), Parallel Computing Technologies. XIV, 635 pages. 2007.

Vol. 4660: S. Džeroski, J. Todorovski (Eds.), Computational Discovery of Scientific Knowledge. X, 327 pages. 2007. (Sublibrary LNAI).

Vol. 4659: V. Mařík, V. Vyatkin, A.W. Colombo (Eds.), Holonic and Multi-Agent Systems for Manufacturing. VIII, 456 pages. 2007. (Sublibrary LNAI).

Vol. 4658: T. Enokido, L. Barolli, M. Takizawa (Eds.), Network-Based Information Systems. XIII, 544 pages. 2007.

Vol. 4657: C. Lambrinoudakis, G. Pernul, A M. Tjoa (Eds.), Trust and Privacy in Digital Business. XIII, 291 pages. 2007.

Vol. 4656: M.A. Wimmer, J. Scholl, Å. Grönlund (Eds.), Electronic Government. XIV, 450 pages. 2007.

Vol. 4655: G. Psaila, R. Wagner (Eds.), E-Commerce and Web Technologies. VII, 229 pages. 2007.

Vol. 4654: I.Y. Song, J. Eder, T.M. Nguyen (Eds.), Data Warehousing and Knowledge Discovery. XVI, 482 pages. 2007.

Vol. 4653: R. Wagner, N. Revell, G. Pernul (Eds.), Database and Expert Systems Applications. XXII, 907 pages. 2007.

Vol. 4651: F. Azevedo, P. Barahona, F. Fages, F. Rossi (Eds.), Recent Advances in Constraints. VIII, 185 pages. 2007. (Sublibrary LNAI).

Vol. 4649: V. Diekert, M.V. Volkov, A. Voronkov (Eds.), Computer Science – Theory and Applications. XIII, 420 pages. 2007.

Vol. 4647: R. Martin, M. Sabin, J. Winkler (Eds.), Mathematics of Surfaces XII. IX, 509 pages. 2007.

Vol. 4645: R. Giancarlo, S. Hannenhalli (Eds.), Algorithms in Bioinformatics. XIII, 432 pages. 2007. (Sublibrary LNBI).

Vol. 4644: N. Azemard, L. Svensson (Eds.), Integrated Circuit and System Design. XIV, 583 pages. 2007.

Vol. 4643: M.-F. Sagot, M.E.M.T. Walter (Eds.), Advances in Bioinformatics and Computational Biology. XII, 177 pages. 2007. (Sublibrary LNBI).

Vol. 4642: S.-W. Lee, S.Z. Li (Eds.), Advances in Biometrics. XX, 1216 pages. 2007.

Vol. 4641: A.-M. Kermarrec, L. Bougé, T. Priol (Eds.), Euro-Par 2007 Parallel Processing. XXVII, 974 pages. 2007.

Vol. 4639: E. Csuhaj-Varjú, Z. Ésik (Eds.), Fundamentals of Computation Theory. XIV, 508 pages. 2007.

Vol. 4638: T. Stützle, M. Birattari, H.H. Hoos (Eds.), Engineering Stochastic Local Search Algorithms. X, 223 pages. 2007.

Vol. 4637: C. Kruegel, R. Lippmann, A. Clark (Eds.), Recent Advances in Intrusion Detection. XII, 337 pages. 2007.

Vol. 4635: B. Kokinov, D.C. Richardson, T.R. Roth-Berghofer, L. Vieu (Eds.), Modeling and Using Context. XIV, 574 pages. 2007. (Sublibrary LNAI).

Vol. 4634: H.R. Nielson, G. Filé (Eds.), Static Analysis. XI, 469 pages. 2007.

Vol. 4633: M. Kamel, A. Campilho (Eds.), Image Analysis and Recognition. XII, 1312 pages. 2007.

Vol. 4632: R. Alhajj, H. Gao, X. Li, J. Li, O.R. Zaïane (Eds.), Advanced Data Mining and Applications. XV, 634 pages. 2007. (Sublibrary LNAI).

Vol. 4628: L.N. de Castro, F.J. Von Zuben, H. Knidel (Eds.), Artificial Immune Systems. XII, 438 pages. 2007.

Vol. 4627: M. Charikar, K. Jansen, O. Reingold, J.D.P. Rolim (Eds.), Approximation, Randomization, and Combinatorial Optimization. XII, 626 pages. 2007.

Vol. 4626: R.O. Weber, M.M. Richter (Eds.), Case-Based Reasoning Research and Development. XIII, 534 pages. 2007. (Sublibrary LNAI).

Vol. 4624: T. Mossakowski, U. Montanari, M. Haveraaen (Eds.), Algebra and Coalgebra in Computer Science. XI, 463 pages. 2007.

Vol. 4622: A. Menezes (Ed.), Advances in Cryptology - CRYPTO 2007. XIV, 631 pages. 2007.

Vol. 4619: F. Dehne, J.-R. Sack, N. Zeh (Eds.), Algorithms and Data Structures. XVI, 662 pages. 2007.

Vol. 4618: S.G. Akl, C.S. Calude, M.J. Dinneen, G. Rozenberg, H.T. Wareham (Eds.), Unconventional Computation. X, 243 pages. 2007.

Vol. 4617: V. Torra, Y. Narukawa, Y. Yoshida (Eds.), Modeling Decisions for Artificial Intelligence. XII, 502 pages. 2007. (Sublibrary LNAI).

Vol. 4616: A. Dress, Y. Xu, B. Zhu (Eds.), Combinatorial Optimization and Applications. XI, 390 pages. 2007.

Vol. 4615: R. de Lemos, C. Gacek, A. Romanovsky (Eds.), Architecting Dependable Systems IV. XIV, 435 pages. 2007.

Vol. 4613: F.P. Preparata, Q. Fang (Eds.), Frontiers in Algorithmics. XI, 348 pages. 2007.

Vol. 4612: I. Miguel, W. Ruml (Eds.), Abstraction, Reformulation, and Approximation. XI, 418 pages. 2007. (Sublibrary LNAI).

Vol. 4611: J. Indulska, J. Ma, L.T. Yang, T. Ungerer, J. Cao (Eds.), Ubiquitous Intelligence and Computing. XXIII, 1257 pages. 2007.

Vol. 4610: B. Xiao, L.T. Yang, J. Ma, C. Muller-Schloer, Y. Hua (Eds.), Autonomic and Trusted Computing. XVIII, 571 pages. 2007.

Vol. 4609: E. Ernst (Ed.), ECOOP 2007 – Object-Oriented Programming. XIII, 625 pages. 2007.

Vol. 4608: H.W. Schmidt, I. Crnkovic, G.T. Heineman, J.A. Stafford (Eds.), Component-Based Software Engineering. XII, 283 pages. 2007.

Vol. 4607: L. Baresi, P. Fraternali, G.-J. Houben (Eds.), Web Engineering. XVI, 576 pages. 2007.

Vol. 4606: A. Pras, M. van Sinderen (Eds.), Dependable and Adaptable Networks and Services. XIV, 149 pages. 2007.

Vol. 4605: D. Papadias, D. Zhang, G. Kollios (Eds.), Advances in Spatial and Temporal Databases. X, 479 pages. 2007.

Vol. 4604: U. Priss, S. Polovina, R. Hill (Eds.), Conceptual Structures: Knowledge Architectures for Smart Applications. XII, 514 pages. 2007. (Sublibrary LNAI).

Vol. 4603: F. Pfenning (Ed.), Automated Deduction – CADE-21. XII, 522 pages. 2007. (Sublibrary LNAI).

Vol. 4602: S. Barker, G.-J. Ahn (Eds.), Data and Applications Security XXI. X, 291 pages. 2007.

Vol. 4600: H. Comon-Lundh, C. Kirchner, H. Kirchner (Eds.), Rewriting, Computation and Proof. XVI, 273 pages. 2007.

Vol. 4599: S. Vassiliadis, M. Berekovic, T.D. Hämäläinen (Eds.), Embedded Computer Systems: Architectures, Modeling, and Simulation. XVIII, 466 pages. 2007.

Vol. 4598: G. Lin (Ed.), Computing and Combinatorics. XII, 570 pages. 2007.

Vol. 4597: P. Perner (Ed.), Advances in Data Mining. XI, 353 pages. 2007. (Sublibrary LNAI).

Vol. 4596: L. Arge, C. Cachin, T. Jurdziński, A. Tarlecki (Eds.), Automata, Languages and Programming. XVII, 953 pages. 2007.

Vol. 4595: D. Bošnački, S. Edelkamp (Eds.), Model Checking Software. X, 285 pages. 2007.

Vol. 4594: R. Bellazzi, A. Abu-Hanna, J. Hunter (Eds.), Artificial Intelligence in Medicine. XVI, 509 pages. 2007. (Sublibrary LNAI).

Vol. 4593: A. Biryukov (Ed.), Fast Software Encryption. XI, 467 pages. 2007.

Vol. 4592: Z. Kedad, N. Lammari, E. Métais, F. Meziane, Y. Rezgui (Eds.), Natural Language Processing and Information Systems. XIV, 442 pages. 2007.

Vol. 4591: J. Davies, J. Gibbons (Eds.), Integrated Formal Methods. IX, 660 pages. 2007.

Vol. 4590: W. Damm, H. Hermanns (Eds.), Computer Aided Verification. XV, 562 pages. 2007.

Vol. 4589: J. Münch, P. Abrahamsson (Eds.), Product-Focused Software Process Improvement. XII, 414 pages. 2007.

Vol. 4588: T. Harju, J. Karhumäki, A. Lepistö (Eds.), Developments in Language Theory. XI, 423 pages. 2007.

Vol. 4587: R. Cooper, J. Kennedy (Eds.), Data Management. XIII, 259 pages. 2007.

Vol. 4586: J. Pieprzyk, H. Ghodosi, E. Dawson (Eds.), Information Security and Privacy. XIV, 476 pages. 2007.

Vol. 4585: M. Kryszkiewicz, J.F. Peters, H. Rybinski, A. Skowron (Eds.), Rough Sets and Intelligent Systems Paradigms. XIX, 836 pages. 2007. (Sublibrary LNAI).

Vol. 4584: N. Karssemeijer, B. Lelieveldt (Eds.), Information Processing in Medical Imaging. XX, 777 pages. 2007.

Table of Contents

Collision Attacks and Fault Analysis

High Speed AES Implementations

Public-Key Cryptography

Implementation Cost of Countermeasures

Security Issues for RF and RFID

Special Purpose Hardware for Cryptanalysis

Side Channel Analysis

Problems and Solutions for Lightweight Devices

A First-Order DPA Attack Against AES in Counter Mode with Unknown Initial Counter

Josh Jaffe

Cryptography Research, Inc.
575 Market Street, suite 2150, San Francisco, CA 94105, USA
josh@cryptography.com

Abstract. Previous first-order differential power analysis (DPA) attacks have depended on knowledge of the target algorithm's input or output. This paper describes a first-order DPA attack against AES in counter mode, in which the initial counter and output values are all unknown.

Keywords: power analysis, SPA, DPA, HO-DPA, AES, counter mode.

1 Introduction

Previous first-order differential power analysis (DPA) attacks have depended on knowledge of the target algorithm's input or output [1][2]. This paper describes a first-order DPA attack against the Advanced Encryption Standard (AES) [3] in counter mode, in which the initial counter, input values, and output values are all unknown.

The attack proceeds as follows. Suppose the input data to an algorithm is unknown, but can be expressed as single secret constant summed with known, variable data. The known, variable part of the data is used to mount a DPA attack, and the secret constant is treated as part of the key to be recovered. The "key" recovered by the DPA attack is then a function of the actual key and the secret constant. The known input values are then combined with the recovered "key" to compute the actual intermediate values produced by the algorithm. The recovered intermediates are then used to carry the attack forward into later rounds, enabling additional DPA attacks to recover the real key.

The attack also addresses the challenges to DPA presented by block ciphers used in counter mode [4]. DPA attacks target secrets when they are mixed with known *variable* quantities. In counter mode only the low-order bits of the input change with each encryption. Hence there are few variable intermediates to target in the first round of a typical block cipher. We demonstrate a method for propagating the attack into later rounds in which more known, variable data is available.

Although counter mode presents additional challenges to DPA attacks, in certain respects it also makes the attack easier. Unlike most first-order DPA attacks, the sequential nature of the counter enables the attack to succeed with

P. Paillier and I. Verbauwhede (Eds.): CHES 2007, LNCS 4727, pp. 1–13, 2007.

only knowledge of the power measurements. Knowledge of input, output, and initial counter values are not required to implement the attack.

1.1 Related Work

Simple power analysis (SPA) attacks have been used to extract portions of keys directly from power traces without requiring knowledge of input messages. Fahn and Pearson used inferential power analysis (IPA), an attack that exploits binary SPA leaks [5]. Mayer-Sommer presented attacks exploiting SPA leaks in high-amplitude power variations [6]. Mangard presented an SPA attack against the AES key expansion step [7]. Messerges et al described SPA attacks on Hamming weight and transition count leaks [8].

Side channel collision attacks were introduced by Dobbertin, and have traditionally targeted SPA leaks using chosen ciphertext [9] [10] [11]. Side channel collision attacks can be adapted to the case in which inputs are known to be successive values of a counter.

High-order differential power analysis (HO-DPA) [12] attacks target a hypothesized key-dependent relationship between data parameters in a computation. Previous work has noted that HO-DPA attacks can be applied to situations in which cipher input values are not known [13].

Fouque and Valette presented the "doubling attack" [14] which exploits the relationship between inputs in successive RSA decryptions to recover the exponent. The attack succeeds despite the fact that the input to the modular exponentiation step is masked by a blinding factor. Messerges presented a second-order DPA attack [15] that defeated a data whitening scheme.

Chari et al [16] and Akkar et al [17] also presented DPA attacks on block ciphers with a "whitening" step.

2 Preliminaries

2.1 Notation

Suppose X and Y are used to denote input and output data of a transformation. (Letters other than X or Y will also be used.) If the transformation is implemented as a sequence of rounds, the input and output of the i^{th} round are denoted by X_i and Y_i.

Within a round, data may be partitioned into bytes for processing. $X_{i,j}$ and $Y_{i,j}$ denote the j^{th} bytes of round data X_i and V_i.

K is used to denote input keys, K_i denotes the i^{th} round key derived from K, and $K_{i,j}$ denotes the j^{th} byte of round key K_i.

Symbols

The symbol '$\oplus$' denotes the bitwise XOR of two n-bit vectors.
The symbol '$+$' denotes the ordinary addition of two numbers.
The symbol '$\circ$' denotes multiplication between two elements of $GF(2^8)$.
The symbol '||' denotes the concatenation of two vectors.