Kefei Chen
Robert Deng
Xuejia Lai
Jianying Zhou (Eds.)

Information Security Practice and Experience

LNCS 3903

Second International Conference, ISPEC 2006
Hangzhou, China, April 2006
Proceedings

Kefei Chen Robert Deng Xuejia Lai
Jianying Zhou (Eds.)

Information Security Practice and Experience

Second International Conference, ISPEC 2006
Hangzhou, China, April 11-14, 2006
Proceedings

Springer

Volume Editors

Kefei Chen
Shanghai Jiaotong University
1954 Hua Shan Road, Shanghai 200030, P.R. China
E-mail: kfchen@sjtu.edu.cn

Robert Deng
Singapore Management University
469 Bukit Timah Road, 259756, Singapore
E-mail: robertdeng@smu.edu.sg

Xuejia Lai
Shanghai Jiaotong University
1954 Hua Shan Road, Shanghai 200030, P.R. China
E-mail: lai-xj@cs.sjtu.edu.cn

Jianying Zhou
Institute for Infocomm Research
21 Heng Mui Keng Terrace, 119613, Singapore
E-mail: jyzhou@i2r.a-star.edu.sg

Library of Congress Control Number: 2006922001

CR Subject Classification (1998): E.3, C.2.0, D.4.6, H.2.0, K.4.4, K.6.5

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743
ISBN-10 3-540-33052-6 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-33052-3 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 11689522 06/3142 5 4 3 2 1 0

Lecture Notes in Computer Science 3903

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. 1–3806

please contact your bookseller or Springer

Vol. 3903: K. Chen, R. Deng, X. Lai, J. Zhou (Eds.), Information Security Practice and Experience. XIV, 392 pages. 2006.

Vol. 3901: P.M. Hill (Ed.), Logic Based Program Synthesis and Transformation. X, 179 pages. 2006.

Vol. 3899: S. Frintrop, VOCUS: A Visual Attention System for Object Detection and Goal-Directed Search. XIV, 216 pages. 2006. (Sublibrary LNAI).

Vol. 3895: O. Goldreich, A.L. Rosenberg, A.L. Selman (Eds.), Essays in Theoretical Computer Science. XII, 399 pages. 2006.

Vol. 3894: W. Grass, B. Sick, K. Waldschmidt (Eds.), Architecture of Computing Systems - ARCS 2006. XII, 496 pages. 2006.

Vol. 3890: S.G. Thompson, R. Ghanea-Hercock (Eds.), Defence Applications of Multi-Agent Systems. XII, 141 pages. 2006. (Sublibrary LNAI).

Vol. 3889: J. Rosca, D. Erdogmus, J.C. Príncipe, S. Haykin (Eds.), Independent Component Analysis and Blind Signal Separation. XXI, 980 pages. 2006.

Vol. 3888: D. Draheim, G. Weber (Eds.), Trends in Enterprise Application Architecture. IX, 145 pages. 2006.

Vol. 3887: J. Correa, A. Hevia, M. Kiwi (Eds.), LATIN 2006: Theoretical Informatics. XVI, 814 pages. 2006.

Vol. 3886: E.G. Bremer, J. Hakenberg, E.-H.(S.) Han, D. Berrar, W. Dubitzky (Eds.), Knowledge Discovery in Life Science Literature. XIV, 147 pages. 2006. (Sublibrary LNBI).

Vol. 3885: V. Torra, Y. Narukawa, A. Valls, J. Domingo-Ferrer (Eds.), Modeling Decisions for Artificial Intelligence. XII, 374 pages. 2006. (Sublibrary LNAI).

Vol. 3884: B. Durand, W. Thomas (Eds.), STACS 2006. XIV, 714 pages. 2006.

Vol. 3881: S. Gibet, N. Courty, J.-F. Kamp (Eds.), Gesture in Human-Computer Interaction and Simulation. XIII, 344 pages. 2006. (Sublibrary LNAI).

Vol. 3880: A. Rashid, M. Aksit (Eds.), Transactions on Aspect-Oriented Software Development I. IX, 335 pages. 2006.

Vol. 3879: T. Erlebach, G. Persinao (Eds.), Approximation and Online Algorithms. X, 349 pages. 2006.

Vol. 3878: A. Gelbukh (Ed.), Computational Linguistics and Intelligent Text Processing. XVII, 589 pages. 2006.

Vol. 3877: M. Detyniecki, J.M. Jose, A. Nürnberger, C. J. '. van Rijsbergen (Eds.), Adaptive Multimedia Retrieval: User, Context, and Feedback. XI, 279 pages. 2006.

Vol. 3876: S. Halevi, T. Rabin (Eds.), Theory of Cryptography. XI, 617 pages. 2006.

Vol. 3875: S. Ur, E. Bin, Y. Wolfsthal (Eds.), Haifa Verification Conference. X, 265 pages. 2006.

Vol. 3874: R. Missaoui, J. Schmidt (Eds.), Formal Concept Analysis. X, 309 pages. 2006. (Sublibrary LNAI).

Vol. 3873: L. Maicher, J. Park (Eds.), Charting the Topic Maps Research and Applications Landscape. VIII, 281 pages. 2006. (Sublibrary LNAI).

Vol. 3872: H. Bunke, A. L. Spitz (Eds.), Document Analysis Systems VII. XIII, 630 pages. 2006.

Vol. 3870: S. Spaccapietra, P. Atzeni, W.W. Chu, T. Catarci, K.P. Sycara (Eds.), Journal on Data Semantics V. XIII, 237 pages. 2006.

Vol. 3869: S. Renals, S. Bengio (Eds.), Machine Learning for Multimodal Interaction. XIII, 490 pages. 2006.

Vol. 3868: K. Römer, H. Karl, F. Mattern (Eds.), Wireless Sensor Networks. XI, 342 pages. 2006.

Vol. 3866: T. Dimitrakos, F. Martinelli, P.Y.A. Ryan, S. Schneider (Eds.), Formal Aspects in Security and Trust. X, 259 pages. 2006.

Vol. 3865: W. Shen, K.-M. Chao, Z. Lin, J.-P.A. Barthès (Eds.), Computer Supported Cooperative Work in Design II. XII, 359 pages. 2006.

Vol. 3863: M. Kohlhase (Ed.), Mathematical Knowledge Management. XI, 405 pages. 2006. (Sublibrary LNAI).

Vol. 3862: R.H. Bordini, M. Dastani, J. Dix, A.E.F. Seghrouchni (Eds.), Programming Multi-Agent Systems. XIV, 267 pages. 2006. (Sublibrary LNAI).

Vol. 3861: J. Dix, S.J. Hegner (Eds.), Foundations of Information and Knowledge Systems. X, 331 pages. 2006.

Vol. 3860: D. Pointcheval (Ed.), Topics in Cryptology – CT-RSA 2006. XI, 365 pages. 2006.

Vol. 3858: A. Valdes, D. Zamboni (Eds.), Recent Advances in Intrusion Detection. X, 351 pages. 2006.

Vol. 3857: M.P.C. Fossorier, H. Imai, S. Lin, A. Poli (Eds.), Applied Algebra, Algebraic Algorithms and Error-Correcting Codes. XI, 350 pages. 2006.

Vol. 3855: E. A. Emerson, K.S. Namjoshi (Eds.), Verification, Model Checking, and Abstract Interpretation. XI, 443 pages. 2005.

Vol. 3854: I. Stavrakakis, M. Smirnov (Eds.), Autonomic Communication. XIII, 303 pages. 2006.

Vol. 3853: A.J. Ijspeert, T. Masuzawa, S. Kusumoto (Eds.), Biologically Inspired Approaches to Advanced Information Technology. XIV, 388 pages. 2006.

Vol. 3852: P.J. Narayanan, S.K. Nayar, H.-Y. Shum (Eds.), Computer Vision – ACCV 2006, Part II. XXXI, 977 pages. 2006.

Vol. 3851: P.J. Narayanan, S.K. Nayar, H.-Y. Shum (Eds.), Computer Vision – ACCV 2006, Part I. XXXI, 973 pages. 2006.

Vol. 3850: R. Freund, G. Păun, G. Rozenberg, A. Salomaa (Eds.), Membrane Computing. IX, 371 pages. 2006.

Vol. 3849: I. Bloch, A. Petrosino, A.G.B. Tettamanzi (Eds.), Fuzzy Logic and Applications. XIV, 438 pages. 2006. (Sublibrary LNAI).

Vol. 3848: J.-F. Boulicaut, L. De Raedt, H. Mannila (Eds.), Constraint-Based Mining and Inductive Databases. X, 401 pages. 2006. (Sublibrary LNAI).

Vol. 3847: K.P. Jantke, A. Lunzer, N. Spyratos, Y. Tanaka (Eds.), Federation over the Web. X, 215 pages. 2006. (Sublibrary LNAI).

Vol. 3846: H. J. van den Herik, Y. Björnsson, N.S. Netanyahu (Eds.), Computers and Games. XIV, 333 pages. 2006.

Vol. 3845: J. Farré, I. Litovsky, S. Schmitz (Eds.), Implementation and Application of Automata. XIII, 360 pages. 2006.

Vol. 3844: J.-M. Bruel (Ed.), Satellite Events at the MoDELS 2005 Conference. XIII, 360 pages. 2006.

Vol. 3843: P. Healy, N.S. Nikolov (Eds.), Graph Drawing. XVII, 536 pages. 2006.

Vol. 3842: H.T. Shen, J. Li, M. Li, J. Ni, W. Wang (Eds.), Advanced Web and Network Technologies, and Applications. XXVII, 1057 pages. 2006.

Vol. 3841: X. Zhou, J. Li, H.T. Shen, M. Kitsuregawa, Y. Zhang (Eds.), Frontiers of WWW Research and Development - APWeb 2006. XXIV, 1223 pages. 2006.

Vol. 3840: M. Li, B. Boehm, L.J. Osterweil (Eds.), Unifying the Software Process Spectrum. XVI, 522 pages. 2006.

Vol. 3839: J.-C. Filliâtre, C. Paulin-Mohring, B. Werner (Eds.), Types for Proofs and Programs. VIII, 275 pages. 2006.

Vol. 3838: A. Middeldorp, V. van Oostrom, F. van Raamsdonk, R. de Vrijer (Eds.), Processes, Terms and Cycles: Steps on the Road to Infinity. XVIII, 639 pages. 2005.

Vol. 3837: K. Cho, P. Jacquet (Eds.), Technologies for Advanced Heterogeneous Networks. IX, 307 pages. 2005.

Vol. 3836: J.-M. Pierson (Ed.), Data Management in Grids. X, 143 pages. 2006.

Vol. 3835: G. Sutcliffe, A. Voronkov (Eds.), Logic for Programming, Artificial Intelligence, and Reasoning. XIV, 744 pages. 2005. (Sublibrary LNAI).

Vol. 3834: D.G. Feitelson, E. Frachtenberg, L. Rudolph, U. Schwiegelshohn (Eds.), Job Scheduling Strategies for Parallel Processing. VIII, 283 pages. 2005.

Vol. 3833: K.-J. Li, C. Vangenot (Eds.), Web and Wireless Geographical Information Systems. XI, 309 pages. 2005.

Vol. 3832: D. Zhang, A.K. Jain (Eds.), Advances in Biometrics. XX, 796 pages. 2005.

Vol. 3831: J. Wiedermann, G. Tel, J. Pokorný, M. Bieliková, J. Štuller (Eds.), SOFSEM 2006: Theory and Practice of Computer Science. XV, 576 pages. 2006.

Vol. 3830: D. Weyns, H. V.D. Parunak, F. Michel (Eds.), Environments for Multi-Agent Systems II. VIII, 291 pages. 2006. (Sublibrary LNAI).

Vol. 3829: P. Pettersson, W. Yi (Eds.), Formal Modeling and Analysis of Timed Systems. IX, 305 pages. 2005.

Vol. 3828: X. Deng, Y. Ye (Eds.), Internet and Network Economics. XVII, 1106 pages. 2005.

Vol. 3827: X. Deng, D.-Z. Du (Eds.), Algorithms and Computation. XX, 1190 pages. 2005.

Vol. 3826: B. Benatallah, F. Casati, P. Traverso (Eds.), Service-Oriented Computing - ICSOC 2005. XVIII, 597 pages. 2005.

Vol. 3824: L.T. Yang, M. Amamiya, Z. Liu, M. Guo, F.J. Rammig (Eds.), Embedded and Ubiquitous Computing – EUC 2005. XXIII, 1204 pages. 2005.

Vol. 3823: T. Enokido, L. Yan, B. Xiao, D. Kim, Y. Dai, L.T. Yang (Eds.), Embedded and Ubiquitous Computing – EUC 2005 Workshops. XXXII, 1317 pages. 2005.

Vol. 3822: D. Feng, D. Lin, M. Yung (Eds.), Information Security and Cryptology. XII, 420 pages. 2005.

Vol. 3821: R. Ramanujam, S. Sen (Eds.), FSTTCS 2005: Foundations of Software Technology and Theoretical Computer Science. XIV, 566 pages. 2005.

Vol. 3820: L.T. Yang, X.-s. Zhou, W. Zhao, Z. Wu, Y. Zhu, M. Lin (Eds.), Embedded Software and Systems. XXVIII, 779 pages. 2005.

Vol. 3819: P. Van Hentenryck (Ed.), Practical Aspects of Declarative Languages. X, 231 pages. 2005.

Vol. 3818: S. Grumbach, L. Sui, V. Vianu (Eds.), Advances in Computer Science – ASIAN 2005. XIII, 294 pages. 2005.

Vol. 3817: M. Faundez-Zanuy, L. Janer, A. Esposito, A. Satue-Villar, J. Roure, V. Espinosa-Duro (Eds.), Nonlinear Analyses and Algorithms for Speech Processing. XII, 380 pages. 2006. (Sublibrary LNAI).

Vol. 3816: G. Chakraborty (Ed.), Distributed Computing and Internet Technology. XXI, 606 pages. 2005.

Vol. 3815: E.A. Fox, E.J. Neuhold, P. Premsmit, V. Wuwongse (Eds.), Digital Libraries: Implementing Strategies and Sharing Experiences. XVII, 529 pages. 2005.

Vol. 3814: M. Maybury, O. Stock, W. Wahlster (Eds.), Intelligent Technologies for Interactive Entertainment. XV, 342 pages. 2005. (Sublibrary LNAI).

Vol. 3813: R. Molva, G. Tsudik, D. Westhoff (Eds.), Security and Privacy in Ad-hoc and Sensor Networks. VIII, 219 pages. 2005.

Vol. 3812: C. Bussler, A. Haller (Eds.), Business Process Management Workshops. XIII, 520 pages. 2006.

Vol. 3811: C. Bussler, M.-C. Shan (Eds.), Technologies for E-Services. VIII, 127 pages. 2006.

Vol. 3810: Y.G. Desmedt, H. Wang, Y. Mu, Y. Li (Eds.), Cryptology and Network Security. XI, 349 pages. 2005.

Vol. 3809: S. Zhang, R. Jarvis (Eds.), AI 2005: Advances in Artificial Intelligence. XXVII, 1344 pages. 2005. (Sublibrary LNAI).

Vol. 3808: C. Bento, A. Cardoso, G. Dias (Eds.), Progress in Artificial Intelligence. XVIII, 704 pages. 2005. (Sublibrary LNAI).

Vol. 3807: M. Dean, Y. Guo, W. Jun, R. Kaschek, S. Krishnaswamy, Z. Pan, Q.Z. Sheng (Eds.), Web Information Systems Engineering – WISE 2005 Workshops. XV, 275 pages. 2005.

Preface

This volume contains the Research Track proceedings of the Second Information Security Practice and Experience Conference 2006 (ISPEC 2006), which took place in Hangzhou, China, April 11–14, 2006. The inaugural ISPEC 2005 was held exactly one year earlier in Singapore.

As applications of information security technologies become pervasive, issues pertaining to their deployment and operations are becoming increasingly important. ISPEC is an annual conference that brings together researchers and practitioners to provide a confluence of new information security technologies, their applications and their integration with IT systems in various vertical sectors.

ISPEC 2006 received 307 submissions. This is probably the highest number of paper submissions in any information security-related technical conferences. Due to this exceptionally large number of submissions and the high quality of the submitted papers, not all the papers that contained innovative ideas could be accepted. Each paper was sent to at least three Program Committee members for comments. Based on the reviewers' comments and discussion by the Program Committee, of the 307 submissions, 35 were selected for inclusion in these proceedings as research track papers and another 21 papers were selected as industrial track papers and are published in the Journal of Shanghai Jiaotong University (Science).

As always, the success of an international conference was made possible through the contributions from many individuals and organizations. We would like to thank all the authors who submitted papers. We are indebted to our Program Committee members and the external reviewers for the great job they did. We sincerely thank our General Chair Xuejia Lai for his support and encouragement, Ying Qiu for managing the website for paper submission, review and notification, Feng Bao for helping out in several "emergency" situations and Jianying Zhou for his excellent work as Publication and Publicity Chair. Our special thanks are due to the members of the Local Organizing Committee at Shanghai Jiaotong University, in particular to Yanfei Zheng, Meiju Chen and Zhihua Su for their great efforts to make the conference run smoothly.

Last but not least, we are grateful to Shanghai Jiaotong University, the Institute for Infocomm Research and Singapore Management University for sponsoring the conference.

January 2006

Kefei Chen
Robert H. Deng

ISPEC 2006

Second Information Security Practice and Experience Conference

Hangzhou, China
April 11-14, 2006

Organized by

Shanghai Jiaotong University, China

Sponsored by

Shanghai Jiaotong University, China
and
Singapore Management University, Singapore
and
Institute for Infocomm Research, Singapore

General Chair

Xuejia Lai ..... Shanghai Jiaotong University, China

Program Chairs

Kefei Chen ..... Shanghai Jiaotong University, China
Robert H. Deng ..... Singapore Management University, Singapore

Publication Chair

Jianying Zhou ..... Institute for Infocomm Research, Singapore

Program Committee

Tuomas Aura ..... Microsoft Research, UK
Feng Bao ..... I2R, Singapore
Chin-Chen Chang ..... CCU, Taiwan
Lily Chen ..... NIST, USA
Liqun Chen ..... HP Bristol Labs, UK
Xiaotie Deng ..... City U. of Hong Kong, Hong Kong, China
Jintai Ding ..... U. of Cincinnati, USA
Xuhua Ding ..... SMU, Singapore

Dengguo Feng ..... Chinese Academy of Sciences, China
Dieter Gollmann ..... TU Hamburg, Germany
Guang Gong ..... U. of Waterloo, Canada
Dawu Gu ..... Shanghai Jiaotong U., China
Yongfei Han ..... Onets, China
Yupu Hu ..... Xidian U., China
Jiwu Huang ..... Sun Yat-Sen U., China
Sushil Jajodia ..... GMU, USA
Kwangjo Kim ..... ICU, Korea
Chi-Sung Laih ..... NCKU, Taiwan
Dong Hoon Lee ..... Korea U., Korea
Ninghui Li ..... Purdue U., USA
Tieyan Li ..... I2R, Singapore
Yingjiu Li ..... SMU, Singapore
Shengli Liu ..... Shanghai Jiaotong U., China
Javier Lopez ..... U. of Malaga, Spain
Jianfeng Ma ..... Xidian U., China
Wenbo Mao ..... HP Lab, China
David Naccache ..... Gemplus, France
Masahiro Mambo ..... U. of Tsukuba, Japan
Chris Mitchell ..... U. of London, UK
SangJae Moon ..... Kyungpook National U., Korea
Hweehwa Pang ..... SMU, Singapore
Reihaneh Safavi-Naini ..... UOW, Australia
Kouichi Sakurai ..... Kyushu U., Japan
Joerg Schwenk ..... Ruhr U. Bochum, Germany
Dawn Song ..... CMU, USA
Vijay Varadharajan ..... Macquarie U., Australia
Serge Vaudenay ..... EPFL, Switzerland
Guilin Wang ..... I2R, Singapore
Victor Wei ..... The Chinese U. of Hong Kong, Hong Kong, China
Wenling Wu ..... Chinese Academy of Sciences, China
Yongdong Wu ..... I2R, Singapore
Bo Yang ..... South China Agricultural University, China
Yiqun Lisa Yin ..... Independent Consultant, USA
Moti Yung ..... Columbia U., USA
Huanguo Zhang ..... Wuhan U, China
Muxiang Zhang ..... Verizon Communications, USA
Yunlei Zhao ..... Fudan U., China
Dong Zheng ..... Shanghai Jiaotong U., China
Yuliang Zheng ..... UNCC, USA
Jianying Zhou ..... I2R, Singapore
Huafei Zhu ..... I2R, Singapore
Yuefei Zhu ..... Information Engineering U., China

External Reviewers

Amit Lakhani, Andre Adelsbach, Angela Piper, Anindo Mukherjee, Anyi Liu, Baodian Wei, Becky Jie Liu, Benoit Chevallier-Mames, Bo Yang, Bo Zhu, Cao Aixia, Chen Hua, Chunhua Pan, Dang Nguyen Duc, David M'Raihi, Dayin Wang, Debin Gao, Divyan M. Konidala, Dongvu Tonien, Duc Liem Vo, Eimear Gallery, Fangguo Zhang, Fei Yan, Gerardo Fernandez, Gildas Avoine, Honggang Hu, HUANG Qiong, Hui Li, Hyunrok Lee, Jae-Gwi Choi, James Newsome, Jason Crampton, Jean Monnerat, Jeffrey Horton, John Bethencourt, John Mao, Joonsang Baek, Jose A. Montenegro, Jose A. Oneiva, Joseph Pamula, Katrin Hoeper, Katrin Hoeper, Ken Giulian, Kenji Imamoto, Kishan Chand Gupta, Lei Hu, Lei Zhang, Leonid Reyzin, Liankuan Zhang, Libin Wang, Lifeng Guo, Lijun Liao, Lingyu Wang, Lionel Victor, Lizhen Yang, Lujo Bauer, Luke McAven, Mark Manulis, Martin Vuagnoux, Matthieu Finiasz, Mi Wen, Michael David, Michael Psarros, Min Gyung Kang, Nam Yul Yu, P. George, Patrick George, Qiang Li, Qingguang Ji, Rodrigo Roman, Ron Steinfeld, Ryuzou Nishi, Sankardas Roy, Satoshi Hada, Scott Contini, Sebastian Gajek, Shiping Chen, Shirley H.C. Cheung, Shuhong Wang, Siamak Fayyaz, Sujing Zhou, Tu Feng, Tzong-Chen Wu, Ulrich Greveler, Ulrich Greveler, Wang Chih-Hung, Wei Han, Weizhong Qiang, Wen-Chung Kuo, Wen-Guey Tzeng, Wenming Lu, Xi Chen, Xiangxue Li, xiaodong lin, Xiaofeng Chen, Xiaoming Sun, Xuan Hong, Yang Tommy Guoming, Yanjiang Yang, Yassir Nawaz, Yongbin Zhou, Yoshiaki Hori, Yoshifumi Ueshige, ZHANG Lei, Zhenfeng Zhang, Zhiguo Wan, ZHONG Xiang, ZHOU Juxiang, ZHU Xusong.

Table of Contents

Cryptoanalysis

Network Security I

Network Security II

Security Protocol

Communication Security

Signature and Key Agreement

Application I

Application II

Cryptographic Techniques

System Security

DPA-Resistant Finite Field Multipliers and Secure AES Design

Yoo-Jin Baek and Mi-Jung Noh

System SW Lab., Samsung Electronics Co., Yongin, 449-711, Korea
{yoojin.baek, mjnoh}@samsung.com

Abstract. The masking method is known to be one of the most powerful algorithmic countermeasures against the first-order differential power attack. This article proposes several new efficient masking algorithms applicable to finite field multipliers. Note that the finite field multiplier (more precisely, the finite field inversion) plays a crucial role in the confusion layer of many block ciphers including AES. The new algorithms are applied to implement AES DPA-securely in hardware and the detailed implementation results are presented.

1 Introduction

The differential power attack (DPA) [5] uses the power consumption data to derive some secret information in a cryptographic device. The primary reason why DPA works is that the power consumption signals from a device are strongly related to the internal state of the device, therefore it may leak crucial information about the keying-parameters involved. In particular, this article adopts the power leakage model that the power consumption information leaks the Hamming weight of the data being processed and considers the first-order DPA which investigates the statistical properties of the power consumption information at each sample time [7]. Various countermeasures against the first-order DPA have been proposed so far and the masking method [6] is known to be one of its most powerful algorithmic countermeasures.

The main idea of the masking method is that before a certain cryptographic operation involving a secret key is performed, the input data is masked using a randomly chosen value so that its Hamming weight looks random to the outside world, which clearly prevents an adversary from performing the first-order DPA.

This article proposes new masking algorithms applicable to finite field multipliers. More precisely, efficient algorithms which solve the following problem are presented:

Masking Problem for the Multiplication in a Finite Field. For a given finite field $\mathrm{GF}(q)$ and $(x', r), (y', s) \in \mathrm{GF}(q) \times \mathrm{GF}(q)$ with $x = x' + r$ and $y = y' + s$, compute $(xy + t, t)$ for a random value $t \in \mathrm{GF}(q)$ with the constraint that the Hamming weight distributions of intermediate results must be independent of x and y. Note that in most applications the field $\mathrm{GF}(q)$ is a binary field, i.e. $q = 2^n$ for some n.

K. Chen et al. (Eds.): ISPEC 2006, LNCS 3903, pp. 1–12, 2006.

The related problem for a finite field inversion could also be considered. However, since the inversion can be realized using multiplications (and some linear functions), it is sufficient to consider the multiplication case.

Previous Works. Much work has been done on solving the above problem (and its related problems) [2, 3, 4, 9, 10, 13, 14]. For example, the work in [2, 4, 14] mainly concerned with solving it in software level. Hence, they use the byte-oriented operations or table-lookup operations in their solutions, so they are not adequate to the hardware implementation (in view of critical path and size). On the other hand, our methods are highly hardware-oriented and mainly use bit-wise operations to reduce the hardware size and the critical path.

The methods presented in [3, 13] use the idea of masking at the gate level. More precisely, to apply the masking method to AES, they first decompose the inversion over $GF(2^8)$ into the operations over $GF(2)$. And, noting that the only non-linear operation in $GF(2)$ is the multiplication, i.e. the AND gate, they tried to devise an efficient masking algorithm for the AND gate. In doing so, they used the following simple identities

$$(x \wedge y) \oplus r_z = (((r_z \oplus (r_x \wedge r_y)) \oplus (r_x \wedge y')) \oplus (r_y \wedge x')) \oplus (x' \wedge y')$$

to get $((x \wedge y) \oplus r_z, r_z)$ [13] and

$$(x \wedge y) \oplus r_z = (\neg y' \wedge ((\neg r_y \wedge r_x) \vee (r_y \wedge x'))) \vee (y' \wedge ((r_y \wedge r_x) \vee (\neg r_y \wedge x')))$$

to get $((x \wedge y) \oplus r_x, r_x)$ [3], given (x', r_x) and (y', r_y) with $x' = x \oplus r_x$ and $y' = y \oplus r_y$, where $\wedge, \vee, \oplus$ and $\neg$ stand for AND, OR, XOR and NOT gates, respectively. Consequently, the methods can be implemented using 4 AND and 4 XOR gates [13] or 4 OR, 4 XOR and 3 NOT gates (or 6 AND, 3 OR and 2 NOT gates) [3] to mask the AND gate. Also, the method in citeTri required an additional random bit r_z in its implementation. On the other hand, our method, restricted to $GF(2)$, requires 4 NAND and 4 XOR gates for securing the AND gate without any additional random bit. Since inserting random values into a hardware circuit requires an additional register and may cause some troublesome implementation issues, our method is expected to be more suitable for real hardware implementations than that in [13]. Also, our method is expected to have the smaller critical path than that of [13]. The solution in [3] is highly comparable to our method in the aspect of hardware size, while the exact comparison is highly depending on the used technology.

The final one [9, 10] has similarity with ours in that it used the binary extension field arithmetics over $GF(2^2)$ or $GF(2^4)$ to mask the inversion over $GF(2^8)$ and it didn't require any additional random value. But, as noted in [9], its critical-path and hardware size are less efficient than that of [13]. Hence, our method is expected to have the smaller size and the lower critical path than the method in [9, 10].

The proposed algorithms are applicable to DPA-resistantly implement any cryptographic algorithms which use finite field multipliers as internal (non-linear) operations. The typical example is AES (Advanced Encryption Standard) [1], to

which the new algorithm is applied to result in DPA-secure AES designs. The detailed implementation results are summarized in this paper.

This paper is organized as follows. Section 2 introduces the finite field arithmetics and the overall architecture of AES. Brief explanations about DPA, the masking method and the related masking problem are given in the same section. The new masking algorithm for finite field multiplications can be found in Section 3. Section 4 presents several ways to apply the proposed algorithm to securely (and efficiently) implement the S-box of AES and the whole AES in hardware. The detailed implementation results are summarized in the same section.

2 Preliminaries

2.1 Finite Field Arithmetics

Many block ciphers including AES make an extensive use of arithmetics over a finite field GF(2^n). This section introduces a brief description of GF(2^n).

Let $f(x)$ be an irreducible polynomial of degree n over GF(2). Then one can construct the finite field GF(2^n) $\simeq$ GF(2)[x]/($f(x)$) as follows: as a set, GF(2^n) consists of 2^n elements, each of which can be uniquely written as a polynomial of degree less than n over GF(2). The addition operation in GF(2^n) is the usual polynomial addition over GF(2) (i.e. the component-wise XORing) and the multiplication is the polynomial multiplication over GF(2), followed by a modular reduction by $f(x)$. For any non-zero $g(x) \in GF(2^n)$, one can find $h(x), k(x) \in$ GF(2)[x] such that

$$g(x)h(x) + f(x)k(x) = 1,$$

using the extended Euclidean algorithm. Then $h(x)$ (mod $f(x)$) is the multiplicative inverse of $g(x)$ in GF(2^n).

2.2 DPA and Masking Method

The differential power attack (DPA), which was first introduced by Kocher et al. in [5], tries to find some secret information from power consumption data obtained during some cryptographic operations. The reasons why DPA works are that 1) physical devices consume a different amount of power when operating on logical 1's compared to operating on logical 0's and 2) in applications such as smart cards, power supply for devices from the outside world makes the power consumption easy to measure. In particular, this paper adopts the power leakage model that the power consumption leaks the Hamming weight information of the data being processed. And, this paper considers the first-order DPA which investigates the statistical properties of power signals at each sample time [7]. In the sequel, DPA stands for the first-order DPA.

DPA is performed as follows: first, power consumption signals for randomly chosen plaintexts are gathered and then the set of corresponding plaintexts is partitioned into two subsets, according to some (guessed) key-dependent bits.