

Eli Biham  
Amr M. Youssef (Eds.)

LNCS 4356

# Selected Areas in Cryptography

13th International Workshop, SAC 2006  
Montreal, Canada, August 2006  
Revised Selected Papers



Springer

TN918.1-53  
S 464  
2006  
Eli Biham Amr M. Youssef (Eds.)

# Selected Areas in Cryptography

13th International Workshop, SAC 2006  
Montreal, Canada, August 17-18, 2006  
Revised Selected Papers



Springer



E2007003563

## Volume Editors

Eli Biham

Technion - Israel Institute of Technology

Computer Science Department

Haifa 32000, Israel

E-mail: biham@cs.technion.ac.il

Amr M. Youssef

Concordia University

Concordia Institute for Information Systems Engineering

1425 René Lévesque Blvd. West, Montreal, Quebec, H3G 1M8, Canada

E-mail: youssef@ciise.concordia.ca

Library of Congress Control Number: 2007935809

CR Subject Classification (1998): E.3, D.4.6, K.6.5, F.2.1-2, C.2, H.4.3

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743

ISBN-10 3-540-74461-4 Springer Berlin Heidelberg New York

ISBN-13 978-3-540-74461-0 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 2007

Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India

Printed on acid-free paper SPIN: 12111787 06/3180 5 4 3 2 1 0

# Lecture Notes in Computer Science

## Sublibrary 4: Security and Cryptology

- Vol. 4734: J. Biskup, J. López (Eds.), Computer Security – ESORICS 2007. XIV, 628 pages. 2007.
- Vol. 4727: P. Paillier, I. Verbauwhede (Eds.), Cryptographic Hardware and Embedded Systems - CHES 2007. XIV, 468 pages. 2007.
- Vol. 4691: T. Dimitrakos, F. Martinelli, P.Y.A. Ryan, S. Schneider (Eds.), Formal Aspects in Security and Trust. VIII, 285 pages. 2007.
- Vol. 4677: A. Aldini, R. Gorrieri (Eds.), Foundations of Security Analysis and Design. VII, 325 pages. 2007.
- Vol. 4657: C. Lambrinoudakis, G. Pernul, A. M. Tjoa (Eds.), Trust and Privacy in Digital Business. XIII, 291 pages. 2007.
- Vol. 4637: C. Krügel, R. Lippmann, A. Clark (Eds.), Recent Advances in Intrusion Detection. XII, 337 pages. 2007.
- Vol. 4622: A. Menezes (Ed.), Advances in Cryptology - CRYPTO 2007. XIV, 631 pages. 2007.
- Vol. 4593: A. Biryukov (Ed.), Fast Software Encryption. XI, 467 pages. 2007.
- Vol. 4586: J. Pieprzyk, H. Ghodosi, E. Dawson (Eds.), Information Security and Privacy. XIV, 476 pages. 2007.
- Vol. 4582: J. López, P. Samarati, J.L. Ferrer (Eds.), Public Key Infrastructure. XI, 375 pages. 2007.
- Vol. 4579: B. M. Hämmerli, R. Sommer (Eds.), Detection of Intrusions and Malware, and Vulnerability Assessment. X, 251 pages. 2007.
- Vol. 4575: T. Takagi, T. Okamoto, E. Okamoto, T. Okamoto (Eds.), Pairing-Based Cryptography – Pairing 2007. XI, 408 pages. 2007.
- Vol. 4521: J. Katz, M. Yung (Eds.), Applied Cryptography and Network Security. XIII, 498 pages. 2007.
- Vol. 4515: M. Naor (Ed.), Advances in Cryptology - EUROCRYPT 2007. XIII, 591 pages. 2007.
- Vol. 4499: Y.Q. Shi (Ed.), Transactions on Data Hiding and Multimedia Security II. IX, 117 pages. 2007.
- Vol. 4464: E. Dawson, D.S. Wong (Eds.), Information Security Practice and Experience. XIII, 361 pages. 2007.
- Vol. 4462: D. Sauveron, K. Markantonakis, A. Bilas, J.-J. Quisquater (Eds.), Information Security Theory and Practices. XII, 255 pages. 2007.
- Vol. 4450: T. Okamoto, X. Wang (Eds.), Public Key Cryptography – PKC 2007. XIII, 491 pages. 2007.
- Vol. 4437: J.L. Camenisch, C.S. Collberg, N.F. Johnson, P. Sallee (Eds.), Information Hiding. VIII, 389 pages. 2007.
- Vol. 4392: S.P. Vadhan (Ed.), Theory of Cryptography. XI, 595 pages. 2007.
- Vol. 4377: M. Abe (Ed.), Topics in Cryptology – CT-RSA 2007. XI, 403 pages. 2006.
- Vol. 4356: E. Bihma, A.M. Youssef (Eds.), Selected Areas in Cryptography. XI, 395 pages. 2007.
- Vol. 4341: P.Q. Nguyen (Ed.), Progress in Cryptology - VIETCRYPT 2006. XI, 385 pages. 2006.
- Vol. 4332: A. Bagchi, V. Atluri (Eds.), Information Systems Security. XV, 382 pages. 2006.
- Vol. 4329: R. Barua, T. Lange (Eds.), Progress in Cryptology - INDOCRYPT 2006. X, 454 pages. 2006.
- Vol. 4318: H. Lipmaa, M. Yung, D. Lin (Eds.), Information Security and Cryptology. XI, 305 pages. 2006.
- Vol. 4307: P. Ning, S. Qing, N. Li (Eds.), Information and Communications Security. XIV, 558 pages. 2006.
- Vol. 4301: D. Pointcheval, Y. Mu, K. Chen (Eds.), Cryptology and Network Security. XIII, 381 pages. 2006.
- Vol. 4300: Y.Q. Shi (Ed.), Transactions on Data Hiding and Multimedia Security I. IX, 139 pages. 2006.
- Vol. 4298: J.K. Lee, O. Yi, M. Yung (Eds.), Information Security Applications. XIV, 406 pages. 2007.
- Vol. 4296: M.S. Rhee, B. Lee (Eds.), Information Security and Cryptology – ICISC 2006. XIII, 358 pages. 2006.
- Vol. 4284: X. Lai, K. Chen (Eds.), Advances in Cryptology – ASIACRYPT 2006. XIV, 468 pages. 2006.
- Vol. 4283: Y.Q. Shi, B. Jeon (Eds.), Digital Watermarking. XII, 474 pages. 2006.
- Vol. 4266: H. Yoshiura, K. Sakurai, K. Rannenberg, Y. Murayama, S.-i. Kawamura (Eds.), Advances in Information and Computer Security. XIII, 438 pages. 2006.
- Vol. 4258: G. Danezis, P. Golle (Eds.), Privacy Enhancing Technologies. VIII, 431 pages. 2006.
- Vol. 4249: L. Goubin, M. Matsui (Eds.), Cryptographic Hardware and Embedded Systems - CHES 2006. XII, 462 pages. 2006.
- Vol. 4237: H. Leitold, E.P. Markatos (Eds.), Communications and Multimedia Security. XII, 253 pages. 2006.
- Vol. 4236: L. Breveglieri, I. Koren, D. Naccache, J.-P. Seifert (Eds.), Fault Diagnosis and Tolerance in Cryptography. XIII, 253 pages. 2006.
- Vol. 4219: D. Zamboni, C. Krügel (Eds.), Recent Advances in Intrusion Detection. XII, 331 pages. 2006.
- Vol. 4189: D. Gollmann, J. Meier, A. Sabelfeld (Eds.), Computer Security – ESORICS 2006. XI, 548 pages. 2006.
- Vol. 4176: S.K. Katsikas, J. López, M. Backes, S. Gritzalis, B. Preneel (Eds.), Information Security. XIV, 548 pages. 2006.

- Vol. 4117: C. Dwork (Ed.), Advances in Cryptology - CRYPTO 2006. XIII, 621 pages. 2006.
- Vol. 4116: R. De Prisco, M. Yung (Eds.), Security and Cryptography for Networks. XI, 366 pages. 2006.
- Vol. 4107: G. Di Crescenzo, A. Rubin (Eds.), Financial Cryptography and Data Security. XI, 327 pages. 2006.
- Vol. 4083: S. Fischer-Hübner, S. Furnell, C. Lambri-noudakis (Eds.), Trust and Privacy in Digital Business. XIII, 243 pages. 2006.
- Vol. 4064: R. Büschkes, P. Laskov (Eds.), Detection of Intrusions and Malware & Vulnerability Assessment. X, 195 pages. 2006.
- Vol. 4058: L.M. Batten, R. Safavi-Naini (Eds.), Informa-tion Security and Privacy. XII, 446 pages. 2006.
- Vol. 4047: M.J.B. Robshaw (Ed.), Fast Software Encryp-tion. XI, 434 pages. 2006.
- Vol. 4043: A.S. Atzeni, A. Lioy (Eds.), Public Key In-frastructure. XI, 261 pages. 2006.
- Vol. 4004: S. Vaudenay (Ed.), Advances in Cryptology - EUROCRYPT 2006. XIV, 613 pages. 2006.
- Vol. 3995: G. Müller (Ed.), Emerging Trends in Infor-mation and Communication Security. XX, 524 pages. 2006.
- Vol. 3989: J. Zhou, M. Yung, F. Bao (Eds.), Applied Cryp-tography and Network Security. XIV, 488 pages. 2006.
- Vol. 3969: Ø. Ytrehus (Ed.), Coding and Cryptography. XI, 443 pages. 2006.
- Vol. 3958: M. Yung, Y. Dodis, A. Kiayias, T.G. Malkin (Eds.), Public Key Cryptography - PKC 2006. XIV, 543 pages. 2006.
- Vol. 3957: B. Christianson, B. Crispo, J.A. Malcolm, M. Roe (Eds.), Security Protocols. IX, 325 pages. 2006.
- Vol. 3956: G. Barthe, B. Grégoire, M. Huisman, J.-L. Lanet (Eds.), Construction and Analysis of Safe, Secure, and Interoperable Smart Devices. IX, 175 pages. 2006.
- Vol. 3935: D.H. Won, S. Kim (Eds.), Information Se-curity and Cryptology - ICISC 2005. XIV, 458 pages. 2006.
- Vol. 3934: J.A. Clark, R.F. Paige, F.A.C. Polack, P.J. Brooke (Eds.), Security in Pervasive Computing. X, 243 pages. 2006.
- Vol. 3928: J. Domingo-Ferrer, J. Posegga, D. Schreck-ling (Eds.), Smart Card Research and Advanced Appli-cations. XI, 359 pages. 2006.
- Vol. 3919: R. Safavi-Naini, M. Yung (Eds.), Digital Rights Management. XI, 357 pages. 2006.
- Vol. 3903: K. Chen, R. Deng, X. Lai, J. Zhou (Eds.), Information Security Practice and Experience. XIV, 392 pages. 2006.
- Vol. 3897: B. Preneel, S. Tavares (Eds.), Selected Areas in Cryptography. XI, 371 pages. 2006.
- Vol. 3876: S. Halevi, T. Rabin (Eds.), Theory of Cryp-tography. XI, 617 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. 3860: D. Pointcheval (Ed.), Topics in Cryptology - CT-RSA 2006. XI, 365 pages. 2006.
- Vol. 3858: A. Valdes, D. Zamboni (Eds.), Recent Ad-vances in Intrusion Detection. X, 351 pages. 2006.
- Vol. 3856: G. Danezis, D. Martin (Eds.), Privacy En-hancing Technologies. VIII, 273 pages. 2006.
- Vol. 3786: J.-S. Song, T. Kwon, M. Yung (Eds.), Infor-mation Security Applications. XI, 378 pages. 2006.
- Vol. 3108: H. Wang, J. Pieprzyk, V. Varadharajan (Eds.), Information Security and Privacy. XII, 494 pages. 2004.
- Vol. 2951: M. Naor (Ed.), Theory of Cryptography. XI, 523 pages. 2004.
- Vol. 2742: R.N. Wright (Ed.), Financial Cryptography. VIII, 321 pages. 2003.

We would also like to acknowledge Sheryl Tablan and Sheila Anderson for their great help in the local organization.

Finally, but most importantly, we would like to thank all the authors from all over the world who submitted papers to the workshop, and to all the participants at the workshop.

October 2006

Eli Biham  
Amr Youssef

## Preface

These are the proceedings of SAC 2006, the thirteenth annual workshop on Selected Areas in Cryptography. The workshop was sponsored by the Concordia Institute for Information Systems Engineering, in cooperation with the IACR, the International Association of Cryptologic Research, [www.iacr.org](http://www.iacr.org). This year's themes for SAC were:

1. Design and analysis of symmetric key cryptosystems
2. Primitives for symmetric key cryptography, including block and stream ciphers, hash functions, and MAC algorithms
3. Efficient implementations of symmetric and public key algorithms
4. Side-channel analysis (DPA, DFA, Cache analysis, etc.)

A total of 25 papers were accepted for presentation at the workshop, out of 86 papers submitted (of which one was withdrawn by the authors shortly after the submission deadline). These proceedings contain revised versions of the accepted papers. In addition two invited talks were given: Adi Shamir gave the Stafford Tavares Lecture, entitled "A Top View of Side Channels". The second invited talk was given by Serge Vaudenay entitled "When Stream Cipher Analysis Meets Public-Key Cryptography" (his paper on this topic is enclosed in these proceedings).

The reviewing process was a challenging task, and many good submissions had to be rejected. Each paper was reviewed by at least three members of the Program Committee, and papers co-authored by a member of the Program Committee were reviewed by at least five (other) members. The reviews were then followed by deep discussions on the papers, which contributed a lot to the quality of the final selection. In most cases, extensive comments were sent to the authors. A total of about 300 reviews were written by the committee and external reviewers for the 86 papers, of which 92 reviews were made by 65 external reviewers. Over 240 discussion comments were made by committee members (with up to 30 comments per member). Several papers had deep discussions with 17–19 discussion comments each. In addition, the Co-chairs wrote over 200 additional discussion comments.

It was a pleasure for us to work with the Program Committee, whose members worked very hard during the review process. We are also very grateful to the external referees, who contributed with their special expertise to the selection process. Their work is highly appreciated.

The submission and review process was done using an electronic submission and review software written by Thomas Baignères and Matthieu Finiasz. Thomas and Matthieu also modified and improved their system especially for SAC 2006, with many new features. Their response was very quick and timely, and in many cases features were added or changes were made within less than an hour. We wish to thank them very much for all this work.

# SAC 2006

August 17–18, 2006, Montréal, Canada

Sponsored by the  
Concordia Institute for Information Systems Engineering

In cooperation with the  
*International Association of Cryptologic Research (IACR)*

## Workshop Co-chairs

Eli Biham, Computer Science Department, Technion – Israel  
Institute of Technology, Technion City, Haifa 32000, Israel

Amr M. Youssef, Concordia Institute for Information Systems  
Engineering, Concordia University, 1425 René Lévesque Blvd.  
West, Montréal, Quebec, H3G 1T7, Canada

## Program Committee

Carlisle Adams..... University of Ottawa, Canada  
Alex Biryukov..... University of Luxembourg, Luxembourg  
Nicolas Courtois..... Axalto, France  
Orr Dunkelman..... Technion, Israel  
Helena Handschuh..... Spansion, EMEA, France  
Thomas Johansson..... Lund, Sweden  
Antoine Joux..... Université de Versailles St-Quentin-en-Yvelines, France  
Pascal Junod..... Nagravision, Switzerland  
Lars Knudsen..... DTU, Denmark  
Stefan Lucks..... University of Mannheim, Germany  
Bart Preneel..... Katholieke Universiteit Leuven, Belgium  
Matt Robshaw..... France Telecom, France  
Doug Stinson..... University of Waterloo, Canada  
Stafford Tavares..... Queen's University, Canada  
Eran Tromer..... Weizmann Institute of Science, Israel  
Xiaoyun Wang..... Tsinghua University and Shandong University, China  
Michael Wiener..... Cryptographic Clarity, Canada



## External Referees

Frederik Armknecht  
 Thomas Baignères  
 Elad Barkan  
 Lejla Batina  
 Aurélie Bauer  
 Come Berbain  
 Johannes Bloemer  
 Colin Boyd  
 Anne Canteaut  
 Rafi Chen  
 Carlos Cid  
 Jeremy Clark  
 Scott Contini  
 Ivan Damgaard  
 Blandine Debraize  
 Håkan Englund  
 Aleks Essex  
 Matthieu Finiasz  
 Ewan Fleischmann  
 Guillaume Fumaroli  
 Henri Gilbert  
 Martin Hell

Matt Henricksen  
 Jonathan J. Hoch  
 Tetsu Iwata  
 Ulrich Kühn  
 Nathan Keller  
 Matthias Krause  
 Simon Künzli  
 Tanja Lange  
 Joe Lano  
 Stefan Mangard  
 Alexander Maximov  
 Alexander May  
 Alfred Menezes  
 Nele Mentens  
 Brad Metz  
 Marine Minier  
 Jean Monnerat  
 James Muir  
 Sean Murphy  
 Mridul Nandi  
 Gregory Neven  
 Dag Arne Osvik

Pascal Paillier  
 Souradyuti Paul  
 Jan Pelzl  
 Gilles Piret  
 Axel Poschmann  
 Soren S. Thomsen  
 Kazuo Sakiyama  
 Kai Schramm  
 Jean-Pierre Seifert  
 Nigel Smart  
 Heiko Stamer  
 François-Xavier Standaert  
 Dirk Stegemann  
 Emin Tatli  
 Nicolas Theriault  
 Boaz Tsaban  
 Ingrid Verbauwhede  
 Frederik Vercauteren  
 Charlotte Vikkelsoe  
 Christopher Wolf  
 Robert Zuccherato

*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*

# Table of Contents

## Block Cipher Cryptanalysis

Improved DST Cryptanalysis of IDEA .....	1
<i>Eyüp Serdar Ayaz and Ali Aydın Selçuk</i>	
Improved Related-Key Impossible Differential Attacks on Reduced-Round AES-192 .....	15
<i>Wentao Zhang, Wenling Wu, Lei Zhang, and Dengguo Feng</i>	
Related-Key Rectangle Attack on the Full SHACAL-1 .....	28
<i>Orr Dunkelman, Nathan Keller, and Jongsung Kim</i>	

## Stream Cipher Cryptanalysis I

Cryptanalysis of Achterbahn-Version 2 .....	45
<i>Martin Hell and Thomas Johansson</i>	
Cryptanalysis of the Stream Cipher ABC v2 .....	56
<i>Hongjun Wu and Bart Preneel</i>	

## Block and Stream Ciphers

The Design of a Stream Cipher LEX .....	67
<i>Alex Biryukov</i>	
Dial <b>C</b> for Cipher .....	76
<i>Thomas Baignères and Matthieu Finiasz</i>	
Improved Security Analysis of XEX and LRW Modes .....	96
<i>Kazuhiko Minematsu</i>	

## Side-Channel Attacks

Extended Hidden Number Problem and Its Cryptanalytic Applications .....	114
<i>Martin Hlaváč and Tomáš Rosa</i>	
Changing the Odds Against Masked Logic .....	134
<i>Kris Tiri and Patrick Schaumont</i>	
Advances on Access-Driven Cache Attacks on AES .....	147
<i>Michael Neve and Jean-Pierre Seifert</i>	

Blind Differential Cryptanalysis for Enhanced Power Attacks ..... 163  
*Helena Handschuh and Bart Preneel*

**Efficient Implementations I**

Efficient Implementations of Multivariate Quadratic Systems ..... 174  
*Côme Berbain, Olivier Billet, and Henri Gilbert*

Unbridle the Bit-Length of a Crypto-coprocessor with Montgomery  
Multiplication ..... 188  
*Masayuki Yoshino, Katsuyuki Okeya, and Camille Vuillaume*

Delaying and Merging Operations in Scalar Multiplication: Applications  
to Curve-Based Cryptosystems ..... 203  
*Roberto Maria Avanzi*

**Stream Cipher Cryptanalysis II**

On the Problem of Finding Linear Approximations and Cryptanalysis  
of Pomaranch Version 2 ..... 220  
*Martin Hell and Thomas Johansson*

Multi-pass Fast Correlation Attack on Stream Ciphers ..... 234  
*Bin Zhang and Dengguo Feng*

Crossword Puzzle Attack on NLS ..... 249  
*Joo Yeon Cho and Josef Pieprzyk*

**Invited Talk**

When Stream Cipher Analysis Meets Public-Key Cryptography ..... 266  
*Matthieu Finiasz and Serge Vaudenay*

**Efficient Implementations II**

On Redundant  $\tau$ -Adic Expansions and Non-adjacent Digit Sets ..... 285  
*Roberto Maria Avanzi, Clemens Heuberger, and Helmut Prodinger*

Pairing Calculation on Supersingular Genus 2 Curves ..... 302  
*Colm Ó hÉigearthaigh and Michael Scott*

Efficient Divisor Class Halving on Genus Two Curves ..... 317  
*Peter Birkner*

**Message Authentication Codes**

Message Authentication on 64-Bit Architectures ..... 327  
*Ted Krovetz*

Some Notes on the Security of the Timed Efficient Stream Loss-Tolerant Authentication Scheme .....	342
<i>Goce Jakimoski</i>	

## Hash Functions

Constructing an Ideal Hash Function from Weak Ideal Compression Functions .....	358
<i>Moses Liskov</i>	
Provably Good Codes for Hash Function Design .....	376
<i>Charanjit S. Jutla and Anindya C. Patthak</i>	
<b>Author Index</b> .....	395

# Improved DST Cryptanalysis of IDEA

Eyüp Serdar Ayaz and Ali Aydın Selçuk

Department of Computer Engineering  
Bilkent University  
Ankara, 06800, Turkey  
{serdara,selcuk}@cs.bilkent.edu.tr

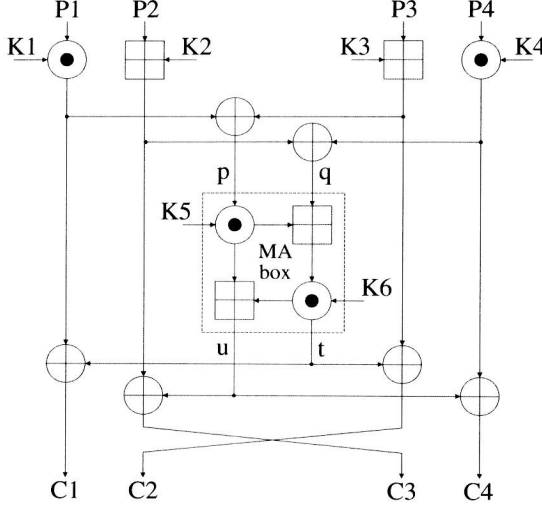
**Abstract.** In this paper, we show how the Demirci-Selcuk-Türe attack, which is currently the deepest penetrating attack on the IDEA block cipher, can be improved significantly in performance. The improvements presented reduce the attack's plaintext, memory, precomputation time, and key search time complexities. These improvements also make a practical implementation of the attack on reduced versions of IDEA possible, enabling the first experimental verifications of the DST attack.

## 1 Introduction

International Data Encryption Algorithm (IDEA) is one of the most popular block ciphers today, commonly used in popular software applications such as PGP. IDEA is known to be extremely secure too: Despite its relatively long history and numerous attempts to analyze it [1, 2, 3, 4, 5, 6, 8, 9, 10, 13, 14, 15], most known attacks on IDEA, which is an 8.5-round cipher, apply to no more than the cipher reduced to 4 rounds. The most effective attack currently known is due to Demirci, Selçuk, and Türe (DST) [7], which is a chosen plaintext attack effective on IDEA up to 5 rounds.

In this paper, we study the ways of enhancing the DST attack and improving its performance. The improvements discussed include shortening the variable part of the plaintexts, reducing the sieving set size, and utilizing previously unused elimination power of the sieving set. The improvements result in a reduction in the plaintext, memory, precomputation time, and key search time complexities of the attack and show that the DST attack can be conducted significantly more efficiently than it was originally thought.

The rest of this paper is organized as follows: In Section 2, we briefly describe the IDEA block cipher. In Section 3, we give an overview of the DST attack. In Section 4, we present several key observations on the DST attack and how to optimize the attack accordingly. In Section 5, we analyze the success probability of the attack according to these optimizations. In Section 6, we present our experimental results and compare them with our theoretical expectations. In Section 7, we calculate the total complexity of the revised attack. Finally in Section 8, we conclude with an overall assessment of the work presented.



**Fig. 1.** One round of IDEA

### 1.1 Notation

We use the following notation in this paper: For modular addition and modular subtraction we use the symbols  $\boxplus$  and  $\boxminus$  respectively. Bitwise exclusive-or (XOR) is denoted by  $\oplus$  and the IDEA multiplication is denoted by  $\odot$ . The plaintext is shown as  $(P_1, P_2, P_3, P_4)$  which is a concatenation of four 16-bit subblocks. Similarly the ciphertext is shown as  $(C_1, C_2, C_3, C_4)$ . The superscripts in parenthesis denote the round numbers. There are six round-key subblocks for each round which are denoted by  $K_1, K_2, K_3, K_4, K_5, K_6$ . The inputs of the MA-box are denoted by  $p$  and  $q$  and the outputs are denoted by  $u$  and  $t$ .

The least significant bit of a variable  $x$  is denoted by  $\text{lsb}(x)$ , the  $i$ th least significant bit is denoted by  $\text{lsb}_i(x)$ , and the least significant  $i$  bits are denoted by  $\text{lsbs}_i(x)$ . Similarly, the most-significant counterparts of these operators are respectively denoted by  $\text{msb}(x)$ ,  $\text{msb}_i(x)$ , and  $\text{msbs}_i(x)$ . Concatenation of two variables  $x, y$  is denoted by  $(x|y)$ . Finally, an inclusive bit interval between the  $m$ th and  $n$ th bits of a round-key subblock  $K_j^{(i)}$  is denoted by  $K_j^{(i)}[m \dots n]$ .

## 2 IDEA Block Cipher

The IDEA block cipher is a modified version of the PES block cipher [11, 12]. IDEA has 64-bit blocks and takes 128-bit keys. The blocks are divided into four 16-bit words and all the operations are on these words. Three different “incompatible” group operations are performed on these words: Bitwise XOR, modular addition, and the *IDEA multiplication*, which is multiplication modulo  $2^{16} + 1$  where 0 represents  $2^{16}$ .

There are two parts in an IDEA round. The first is the transformation part:

$$T : (P_1, P_2, P_3, P_4) \rightarrow (P_1 \odot K_1, P_2 \boxplus K_2, P_3 \boxplus K_3, P_4 \odot K_4).$$

In the second part, two inputs of the MA-box are calculated as  $p = (P_1 \odot K_1) \oplus (P_3 \boxplus K_3)$  and  $q = (P_2 \boxplus K_2) \oplus (P_4 \odot K_4)$ . The outputs of the MA-box are  $t = ((p \odot K_5) \boxplus q) \odot K_6$  and  $u = (p \odot K_5) \boxplus t$ . After these calculations  $t$  is XORed with the first and third output of the transformation part and  $u$  is XORed with the second and fourth. Finally, the ciphertext is formed by taking the outer blocks directly and exchanging the inner blocks.

$$\begin{aligned} C_1 &= (P_1 \odot K_1) \oplus t, \\ C_2 &= (P_3 \boxplus K_3) \oplus t, \\ C_3 &= (P_2 \boxplus K_2) \oplus u, \\ C_4 &= (P_4 \odot K_4) \oplus u. \end{aligned}$$

IDEA consists of eight full rounds and an additional half round, which consists of one transformation part.

The key schedule creates 16-bit round subkeys from a 128-bit master key by taking 16 bits for a subkey and shifting the master key 25 bits after every 8th round key.

Decryption can be done using the encryption algorithm with the multiplicative and additive inverses of the round key subblocks in the transformation part and the same key subblocks in the MA-box.

### 3 The DST Attack

In this section, we give a brief overview of the DST attack with the relevant properties of the IDEA cipher.

#### 3.1 Some Properties of IDEA

The following are some key observations of Demirci et al. [7] on the IDEA cipher which are fundamental to the DST attack. Proofs can be found in the original paper [7].

**Theorem 1.** *Let  $\mathcal{P} = \{(P_1, P_2, P_3, P_4)\}$  be a set of 256 plaintexts such that*

- $P_1, P_3, \text{lsbs}_8(P_2)$  are fixed,
- $\text{msbs}_8(P_2)$  takes all possible values over  $0, 1, \dots, 255$ ,
- $P_4$  varies according to  $P_2$  such that  $q = (P_2 \boxplus K_2^{(1)}) \oplus (P_4 \odot K_4^{(1)})$  is fixed.

*For  $p^{(2)}$  denoting the first input of the MA-box in the second round, the following properties will hold in the encryption of the set  $\mathcal{P}$ :*

- $\text{lsbs}_8(p^{(2)})$  is fixed,
- $\text{msbs}_8(p^{(2)})$  takes all possible values over  $0, 1, \dots, 255$ .



Moreover, the  $p^{(2)}$  values, when ordered according to the plaintext's  $\text{msbs}_8(P_2)$  beginning with  $\text{msbs}_8(P_2) = 0$ , will be of the form

$$(y_0|z), (y_1|z), \dots, (y_{255}|z)$$

for some fixed, 8-bit  $z$ , and  $y_i = (((i \boxplus a) \oplus b) \boxplus c) \oplus d$ , for  $0 \leq i \leq 255$  and fixed, 8-bit  $a, b, c, d$ .

**Theorem 2.** In the encryption of the plaintext set  $\mathcal{P}$  defined in Theorem 1,  $\text{lsb}(K_5^{(2)} \odot p^{(2)})$  equals either  $\text{lsb}(C_2^{(2)} \oplus C_3^{(2)})$  or  $\text{lsb}(C_2^{(2)} \oplus C_3^{(2)}) \oplus 1$  for all the 256 plaintexts in  $\mathcal{P}$ .

**Lemma 1.** In the IDEA round function, the following property is satisfied:

$$\text{lsb}(t \oplus u) = \text{lsb}(p \odot K_5).$$

**Corollary 1.**  $\text{lsb}(C_2^{(i)} \oplus C_3^{(i)} \oplus (K_5^{(i)} \odot (C_1^{(i)} \oplus C_2^{(i)}))) = \text{lsb}(C_2^{(i-1)} \oplus C_3^{(i-1)} \oplus K_2^{(i)} \oplus K_3^{(i)})$ .

**Corollary 2.**  $\text{lsb}(C_2^{(i)} \oplus C_3^{(i)} \oplus (K_5^{(i)} \odot (C_1^{(i)} \oplus C_2^{(i)}))) \oplus (K_5^{(i-1)} \odot (C_1^{(i-1)} \oplus C_2^{(i-1)}))) = \text{lsb}(C_2^{(i-2)} \oplus C_3^{(i-2)} \oplus K_2^{(i)} \oplus K_3^{(i)} \oplus K_2^{(i-1)} \oplus K_3^{(i-1)})$ .

### 3.2 Attack on 3-Round IDEA

The DST attack starts with a precomputation phase where a “sieving set” is prepared which consists of  $2^{56}$  elements of 256-bit strings

$$S = \{f(a, b, c, d, z, K_5^{(2)}) : 0 \leq a, b, c, d, z < 2^8, 0 \leq K_5^{(2)} < 2^{16}\}.$$

computed bitwise as

$$f(a, b, c, d, z, K_5^{(2)})[i] = \text{lsb}(K_5^{(2)} \odot (y_i|z))$$

for  $0 \leq i < 255$ , where  $y_i = (((i \boxplus a) \oplus b) \boxplus c) \oplus d$ .

Once preparation of the sieving set is completed, the main phase of the attack follows. Below is a description of the basic attack on the 3-round IDEA:

1. The attacker takes a chosen plaintext set  $\mathcal{R} = \{(P_1, P_2, P_3, P_4)\}$ , where  $P_1$ ,  $P_3$ , and  $\text{lsbs}_8(P_2)$  are fixed at an arbitrary value, and  $\text{msbs}_8(P_2)$  and  $P_4$  take all possible values. All elements of  $\mathcal{R}$  are encrypted with the 3-round IDEA.
2. For each value of  $K_2^{(1)}$  and  $K_4^{(1)}$ , take a subset  $\mathcal{P}$  of 256 plaintexts from  $\mathcal{R}$  such that  $\text{msbs}_8(P_2)$  varies from 0 to 255 and  $P_4$  is chosen to make  $(P_2 \boxplus K_2^{(1)}) \oplus (P_4 \odot K_4^{(1)})$  constant.
3. For each value of  $K_5^{(3)}$ , a 256-bit string is formed by computing

$$\text{lsb}(C_2^{(3)} \oplus C_3^{(3)} \oplus (K_5^{(3)} \odot (C_1^{(3)} \oplus C_2^{(3)})))$$

for each of the plaintexts in  $\mathcal{P}$ , ordered by  $\text{msbs}_8(P_2)$ . If the current  $(K_2^{(1)}, K_4^{(1)}, K_5^{(3)})$  triple is correct, this 256-bit string must be found in the sieving set. If it cannot be found, the key triple is eliminated.