

Curriculum Vitae

Orr Dunkelman

Updated: April 2011

Department of Computer Science Tel:+972-4-828-8447, +972-54-529-1912
 University of Haifa Fax: +972-4-824-9331
 Haifa 31905 Email: orrd@cs.haifa.ac.il
 Israel Web page: <http://www.cs.haifa.ac.il/~orrd/me>
 Born: Israel, 2th of December, 1980 Family status: Married
 Citizenship: Israeli

Research and Professional Experience

Departement of Computer Science – University of Haifa Feb. 2011–*present*
 Lecturer (tenure-track) position,

Faculty of Mathematics and Computer Science – WEIZMANN INSTITUTE OF SCIENCE Feb. 2011–*present*
 Associated researcher.

Faculty of Mathematics and Computer Science – WEIZMANN INSTITUTE OF SCIENCE Oct. 2009–Jan. 2011
 Post-doctoral research position.

Département d'Informatique – ÉCOLE NORMALE SUPÉRIEURE Apr. 2008–Sep. 2009
 Post-doctoral research position.
 – Part of the ECRYPT research effort (Mar. 2008–Mar. 2008).

Dept. Elektrotechniek-ESAT SCD/COSIC – KATHOLIEKE UNIVERSITEIT LEUVEN Oct. 2006–Mar. 2008
 Post-doctoral research position.
 – Part of the ECRYPT research effort (Oct. 2006–Mar. 2008).

TECHNION – ISRAEL INSTITUTE OF TECHNOLOGY Jun. 1998–Oct. 2006
 Research as part of the Ph.D. studies.
 – Part of the NESSIE research effort (Feb. 2000–Mar. 2003).

Research Interests

Cryptanalysis of symmetric key primitives: block ciphers, stream ciphers, and hash functions.
 Cryptanalysis methods and techniques.
 Design methodologies for symmetric key primitives.
 Linear numerical analysis over finite fields (iterative methods).
 Privacy in the digital world.
 Computer security.

Education

TECHNION – ISRAEL INSTITUTE OF TECHNOLOGY

Ph.D. in Computer Science. Mar. 2000–Feb. 2006
 Dissertation: Techniques for Cryptanalysis of Block Ciphers
 Studies in the direct program towards Ph.D., formal enrollment Feb. 2002.
 Advisor: Prof. Eli Biham Average: 91.4

TECHNION – ISRAEL INSTITUTE OF TECHNOLOGY

B.A. in Computer Science. Oct. 1997–Mar. 2000
 Studies in the Technion's excellence program
 Graduated summa cum laude Average: 91.5

Teaching Experience

LECTURER Oct. 2003–Oct. 2006 & Mar. 2010–*present*

Introduction to Cryptography (203.3444/203.4444) at the University of Haifa

– Spring 2011 (lecturer in charge)

Design and Analysis of Hash Functions at the Weizmann institute of Science

– Winter 2010/11 (along with Prof. Shamir)

Secret Key Cryptography and Cryptanalysis at the Weizmann institute of Science

– Spring 2010 (along with Prof. Shamir)

Advanced Topics in Computer Security (236602) at the Technion

– Winter 2005/6 (lecturer in charge: Prof. Biham)

Computer Security (236350) at the Technion

– Spring 2010 (lecturer in charge: Dr. Bitan)

– Spring 2006 (lecturer in charge)

– Spring 2005 (lecturer in charge: Prof. Biham)

– Winter 2004/5 (lecturer in charge: Dr. Bitan)

– Spring 2004 (lecturer in charge: Dr. Bitan)

– Winter 2003/4 (lecturer in charge: Dr. Bitan)

TEACHING ASSISTANT

Oct. 1999–Oct. 2003

Modern Cryptology (236506) at the Technion

– Winter 2002/3 (lecturer in charge: Prof. Biham)

– Winter 2001/2 (lecturer in charge: Prof. Biham)

– Winter 2000/1 (lecturer in charge: Prof. Biham)

– Winter 1999/2000 (lecturer in charge: Prof. Even)

Advanced Topics in Cryptology at the Technion

– Spring 2003 (236612, lecturer in charge: Prof. Biham)

– Spring 2002 (236612, lecturer in charge: Prof. Biham)

– Spring 2001 (236612, lecturer in charge: Prof. Biham)

– Spring 2000 (236606, lecturer in charge: Prof. Biham)

Numerical Analysis 2 (236320) at the Technion

– Spring 2003 (exercise checking, lecturer in charge: Prof. Sidi)

– Spring 2002 (exercise checking, lecturer in charge: Prof. Sidi)

Computer Security (236350) at the Technion

– Spring 2003 (lecturer in charge: Dr. Bitan)

SCHOOL TEACHER

Oct. 1998–Jun. 1999

Ha'reali school, Haifa, Israel

Tutoring mathematics and cryptography for gifted children.

Honors and Awards

Teaching Awards

Distinguished Lecturer (Technion) — Spring 2010	2010
Distinguished Lecturer (Technion) — Spring 2006	2006
Excellent Teaching Assistant Award	2003

Post-Doctoral Fellowships

Clore Post-Doctoral Fellowship	2010–2011
France Telecom Chaire	2008–2009
KUL — post doctoral grant	2007–2008
Rothschild Post-Doctoral Fellowship	2006–2007

Graduate Studies

Clore Ph.D. Scholarship	2003–2006
Excellence Scholarship	2000

Undergraduate Studies

Technion — President's award for distinction (4 times)	1997–2000
Technion — Dean's list of honor	1999

High School

Youth Mathematics Olympic (Weizmann Institute) — Honors certificate	1997
The 18th International Mathematical Tournament of the Towns — Honors certificate	1997
The Givataim award for excellence in community service	1995

Steering Committees

2008–2013	Selected Areas in Cryptography workshop board
2009–2012	Fast Software Encryption steering committee

Editorial Boards

2009– <i>present</i>	International Journal of Applied Cryptography (IJACT)
2010– <i>present</i>	International Journal of Computer Mathematics (JCOM)

Project Reviewer for

- 1 **Binational (US-Israel) Science Foundation**
- 2 **US National Science Foundation**
- 3 **Research Foundation Flanders (FWO)**

Invited Panelist

- 1 “SHA-256: A Suitable Replacement for SHA-1?” in NIST's cryptographic hash workshop — held in NIST's headquarters, Maryland, USA, 31/10/05

Invitation-Only Workshops (and talks given at them)

Dagstuhl Seminar for Symmetric Key (Jan. 2007)	<i>A Unified Approach for Related Key Attacks</i>
Echternach (Jan. 2008)	<i>Improved Meet-in-the-Middle Attacks on Reduced-Round DES</i>
	<i>What is the Best Attack?</i>
Lorentz Center (June 2008)	<i>Re-Visiting HAIFA and why you should visit too</i>
Dagstuhl Seminar for Symmetric Key (Jan. 2009)	<i>SHAvite-3 - A New and Secure Hash Function Proposal</i>
Early Symmetric Crypto (ESC) 2010 (Jan. 2010)	<i>Attacks of Practical Time Complexity on the A5/3 Underlying Block Cipher</i>
	<i>Low Data Complexity Attacks on AES</i>
	<i>And Now For Something Completely Impossible</i>

Invited Talks

- 1 A Unified Approach to Related-Key Attacks — given at TaiWan Information Security Center (TWISC), Taipei, Taiwan, 11/12/06.
- 2 Combined Attacks for Cryptanalysis of Block Ciphers — given at TaiWan Information Security Center (TWISC), Taipei, Taiwan, 12/12/06.
- 3 Hash Functions — Much Ado about Something — given at Elliptic Curves Cryptography 2008, Utrecht, The Netherlands, 23/9/08.
- 4 New Hash Functions Proposals — given at TaiWan Information Security Center (TWISC), Taipei, Taiwan, 17/11/08.
- 5 Hash Functions — As You Like It — given at TaiWan Information Security Center (TWISC), Taipei, Taiwan, 19/11/08.
- 6 Key Recovery Attacks of Practical Complexity on AES Variants — given at IWCNS 2009, Taipei, Taiwan, 15/12/09.
- 7 The Not So Happily-Ever After End of AES' Security Fairytale — given at CryptoDay 2010 at the Technion, Haifa, Israel, 9/6/10.
- 8 The Hitchhiker's Guide to the SHA-3 Competition — given at Latincrypt 2010, Puebla, Mexico, 10/8/10.

Seminar Talks

- 1 The “Divide and Attack” approach in block cipher cryptanalysis — given at Université Catholique de Louvain, Belgium, 1/2/02.
- 2 First – Divide, Then Attack — given at University of Wollongong, Australia, 27/11/02.
- 3 Trusted Computing — given at IBM's Haifa Research Lab, Israel, 29/6/04.
- 4 The Rectangle Attack — given at Tel Aviv Security Forum (Tausec), Israel, 19/7/05.
- 5 Combined Attacks for Cryptanalysis of Block Ciphers — given at IBM Watson Research Center, New York, 25/8/05.
- 6 Side Channel Attacks — given at IBM's Haifa Research Lab, Israel, 1/5/06.
- 7 New Cryptanalytic Results on IDEA — given at Université Catholique de Louvain, Belgium, 19/12/06.
- 8 Improved Slide Attacks — given at Université Catholique de Louvain, Belgium, 19/12/06.
- 9 New Cryptanalytic Results on IDEA — given at Katholieke Universiteit Leuven, Belgium, 23/2/07.
- 10 Unified Related-Key Attacks — given at École Normale Supérieure, France, 22/5/08.
- 11 Treatment of the Initial Value in Time-Memory-Data Tradeoff Attacks on Stream Ciphers — given at University of Rennes 1, France, 13/6/08.
- 12 Treatment of the Initial Value in Time-Memory-Data Tradeoff Attacks on Stream Ciphers — given at Katholieke Universiteit Leuven, Belgium, 7/7/08.
- 13 Hash Functions — Much Ado about Something — given at University of Wollongong, Australia, 5/12/08.
- 14 Treatment of the Initial Value in Time-Memory-Data Tradeoff Attacks on Stream Ciphers — given at Tel Aviv University, Israel, 8/2/09.
- 15 Traffic Analysis Attacks on a Continuously-Observable Steganographic File System — given at Tel Aviv University, Israel, 9/2/09.
- 16 Treatment of the Initial Value in Time-Memory-Data Tradeoff Attacks on Stream Ciphers — given at University of Haifa, Israel, 11/2/09.
- 17 Traffic Analysis Attacks on a Continuously-Observable Steganographic File System — given at Technion, Israel, 7/4/09.
- 18 KATAN & KTANTAN — A Family of Small and Efficient Hardware-Oriented Block Ciphers — given at Technical university of Graz, Austria, 8/5/09.
- 19 KATAN & KTANTAN — A Family of Small and Efficient Hardware-Oriented Block Ciphers — given at Katholieke Universiteit Leuven, Belgium, 14/9/09.
- 20 Key Recovery Attacks of Practical Complexity on AES Variants — given at École Normale Supérieure, France, 17/9/09.
- 21 Key Recovery Attacks of Practical Complexity on AES Variants — given at University of Rennes 1, France, 25/9/09.

-
- 22 Key Recovery Attacks of Practical Complexity on AES Variants — given at Tel Aviv University, Israel, 29/11/09.
 - 23 Key Recovery Attacks of Practical Complexity on AES Variants — given at Microsoft Research, Seattle, USA, 30/11/09.
 - 24 Key Recovery Attacks of Practical Complexity on AES Variants — given at Technion, Israel, 24/12/09.
 - 25 Key Recovery Attacks of Practical Complexity on AES Variants — given at Haifa University, Israel, 6/1/10.
 - 26 Attacks of Practical Time Complexity on the A5/3 Underlying Block Cipher — given at Tel Aviv University, Israel, 7/1/10.
 - 27 A Practical-Time Attack on the KASUMI Cryptosystem Used in GSM and 3G Telephony — given at Katholieke Universiteit Leuven, Belgium, 7/5/10.
 - 28 A Practical-Time Attack on the KASUMI Cryptosystem Used in GSM and 3G Telephony — given at Ruhr-Universität, Bochum, Germany, 27/5/10.
 - 29 A Practical-Time Related-Key Attack on the KASUMI Cryptosystem Used in GSM and 3G Telephony — given at Microsoft Research, Seattle, USA, 31/8/10.
 - 30 The Hitchhiker's Guide to the SHA-3 Competition — given at Microsoft Research, Seattle, USA, 3/9/10.
 - 31 A Practical-Time Attack on the KASUMI Cryptosystem Used in GSM and 3G Telephony — given at Bonn-Aachen International Center for Information Technology (B-IT), Germany, 16/9/10.

Publications

BOOKS

- 1 O. Dunkelman, editor of *Fast Software Encryptions 2009*, Lecture Notes in Computer Science vol. 5665, Springer, 2009, ISBN 978-3-642-03316-2.
- 2 E. Biham, O. Dunkelman, *Techniques for Cryptanalysis of Block Ciphers*, to appear in 2011, Springer.

JOURNAL PAPERS

- 1 O. Dunkelman, N. Keller, *A New Criterion for Nonlinearity of Block Ciphers*, **IEEE Transactions on Information Theory**, vol. 53, Number 11, pp. 3944–3958, IEEE, 2007.
- 2 O. Dunkelman, N. Keller, *Treatment of the Initial Value in Time-Memory-Data Tradeoff Attacks on Stream Ciphers*, **Information Processing Letters**, vol. 107, No. 5, pp. 133–137, Elsevier, 2008.
- 3 O. Dunkelman, N. Keller, *The Effects of the Omission of Last Round's MixColumns on AES*, **Information Processing Letters**, vol. 110, No. 8–9, pp. 304–308, Elsevier, 2010.
- 4 W. Aerts, E. Biham, D. De Moitie, E. De Mulder, O. Dunkelman, S. Indesteege, N. Keller, B. Preneel, *A Practical Attack on KeeLoq*, accepted to the **Journal of Cryptology**, to appear in 2011.

REFEREED CONFERENCE PROCEEDINGS PAPERS

- 1 E. Biham, A. Biryokuv, O. Dunkelman, E. Richardson, A. Shamir, *Initial Observations on Skipjack: Cryptanalysis of Skipjack-3XOR*, proceedings of **Selected Areas in Cryptography 98**, Lecture Notes in Computer Science, vol. 1556, pp. 362–376, Springer, 1999.
- 2 E. Biham, O. Dunkelman, *Cryptanalysis of the A5/1 GSM Stream Cipher*, proceedings of **INDOCRYPT 2000**, Lecture Notes in Computer Science, vol. 1977, pp. 43–51, Springer, 2000.
- 3 E. Biham, O. Dunkelman, N. Keller, *Linear Cryptanalysis of Reduced Round Serpent*, proceedings of **Fast Software Encryption 2001**, Lecture Notes in Computer Science, vol. 2355, pp. 16–27, Springer, 2002.
- 4 E. Biham, O. Dunkelman, N. Keller, *The Rectangle Attack — Rectangling the Serpent*, proceedings of **EUROCRYPT 2001**, Lecture Notes in Computer Science, vol. 2045, pp. 340–357, Springer, 2001.

-
- 5 E. Biham, O. Dunkelman, N. Keller, *New Results on Boomerang and Rectangle Attack*, proceedings of **Fast Software Encryption 2002**, Lecture Notes in Computer Science, vol. 2365, pp. 1–16, Springer, 2002.
 - 6 H. Yanami, T. Shimoyama, O. Dunkelman, *Differential and Linear Cryptanalysis of Reduced Round SC2000*, proceedings of **Fast Software Encryption 2002**, Lecture Notes in Computer Science, vol. 2365, pp. 34–48, Springer, 2002.
 - 7 E. Biham, O. Dunkelman, N. Keller, *Enhancing Differential-Linear Cryptanalysis*, proceedings of **ASIACRYPT 2002**, Lecture Notes in Computer Science, vol. 2501, pp. 254–266, Springer, 2002.
 - 8 E. Biham, O. Dunkelman, N. Keller, *Differential-Linear Cryptanalysis of Serpent*, proceedings of **Fast Software Encryption 2003**, Lecture Notes in Computer Science, vol. 2887, pp. 9–21, Springer, 2003.
 - 9 E. Biham, O. Dunkelman, N. Keller, *Rectangle Attacks on 49-Round SHACAL-1*, proceedings of **Fast Software Encryption 2003**, Lecture Notes in Computer Science, vol. 2887, pp. 22–35, Springer, 2003.
 - 10 E. Biham, O. Dunkelman, N. Keller, *New Combined Attacks on Block Ciphers*, proceedings of **Fast Software Encryption 2005**, Lecture Notes in Computer Science, vol. 3557, pp. 126–144, Springer, 2005.
 - 11 E. Biham, O. Dunkelman, N. Keller, *Related-Key Boomerang and Rectangle Attacks*, proceedings of **EUROCRYPT 2005**, Lecture Notes in Computer Science vol. 3494, pp. 507–525, Springer, 2005.
 - 12 E. Biham, O. Dunkelman, N. Keller, *Related-Key Rectangle Attack on the Full KASUMI*, proceedings of **ASIACRYPT 2005**, Lecture Notes in Computer Science vol. 3778, pp. 443–461, Springer, 2005.
 - 13 E. Biham, O. Dunkelman, N. Keller, *Related-Key Impossible Differential Attacks on 8-Round AES-192*, proceedings of **CT-RSA 2006**, Lecture Notes in Computer Science vol. 3860, pp. 21–33, Springer, 2006.
 - 14 O. Dunkelman, N. Keller, *A New Criterion for Nonlinearity of Block Ciphers*, proceedings of **CT-RSA 2006**, Lecture Notes in Computer Science vol. 3860, pp. 295–312, Springer, 2006.
 - 15 J. Lu, J. Kim, N. Keller, O. Dunkelman, *Related-Key Rectangle Attack on 42-Round SHACAL-2*, proceedings of **ISC 2006**, Lecture Notes in Computer Science vol. 4176, pp. 85–100, Springer, 2006.
 - 16 O. Dunkelman, N. Keller, J. Kim, *Related-Key Rectangle Attack on the Full SHACAL-1*, proceedings of **Selected Areas in Cryptography 2006**, Lecture Notes in Computer Science vol. 4356, pp. 28–44, Springer, 2007.
 - 17 E. Biham, O. Dunkelman, N. Keller, *New Cryptanalytic Results on IDEA*, proceedings of **ASIACRYPT 2006**, Lecture Notes in Computer Science vol. 4284, pp. 412–427, Springer, 2006.
 - 18 J. Lu, J. Kim, N. Keller, O. Dunkelman, *Differential and Rectangle Attacks on Reduced-Round SHACAL-1*, proceedings of **INDOCRYPT 2006**, Lecture Notes in Computer Science vol. 4329, pp. 17–31, Springer, 2006.
 - 19 E. Biham, O. Dunkelman, N. Keller, *A Simple Related-Key Attack on the Full SHACAL-1*, proceedings of **CT-RSA 2007**, Lecture Notes in Computer Science vol. 4377, pp. 20–30, Springer, 2007.
 - 20 E. Biham, O. Dunkelman, N. Keller, *Improved Slide Attacks*, proceedings of **Fast Software Encryption 2007**, Lecture Notes in Computer Science vol. 4593, pp. 153–166, Springer, 2007.
 - 21 E. Biham, O. Dunkelman, N. Keller, *New Attack on 6-Round IDEA*, proceedings of **Fast Software Encryption 2007**, Lecture Notes in Computer Science vol. 4593, pp. 211–224, Springer, 2007.
 - 22 C. Troncoso, C. Diaz, B. Preneel, O. Dunkelman, *Traffic analysis attacks on a continuously-observable steganographic file system*, proceedings of **Information Hiding 2007**, Lecture Notes in Computer Science vol. 4567, pp. 220–236, Springer, 2007.
 - 23 G. Wang, O. Dunkelman, N. Keller, *The Delicate Issues of Addition with Respect to XOR Differences*, proceedings of **Selected Areas in Cryptography 2007**, Lecture Notes in Computer Science vol. 4876, pp. 212–231, Springer, 2007.

-
- 24 O. Dunkelman, G. Sekar, B. Preneel, *Improved Meet-in-the-Middle Attacks on Reduced-Round DES*, proceedings of **INDOCRYPT 2007**, Lecture Notes in Computer Science vol. 4859, pp. 86–100, Springer, 2007.
 - 25 J. Lu, J. Kim, N. Keller, O. Dunkelman, *Improving the Efficiency of Impossible Differential Cryptanalysis of Reduced Camellia and MISTY1*, proceedings of **CT-RSA 2008**, Lecture Notes in Computer Science vol. 4964, pp. 370–386, Springer, 2008.
 - 26 E. Biham, O. Dunkelman, N. Keller, *A Unified Approach for Related Key Attacks*, proceedings of **Fast Software Encryption 2008**, Lecture Notes in Computer Science vol. 5086, pp. 73–96, Springer, 2008.
 - 27 S. Indestege, N. Keller, O. Dunkelman, E. Biham, B. Preneel, *How to Steal Cars — A Practical Attack on Keeloq*, proceedings of **EUROCRYPT 2008**, Lecture Notes in Computer Science vol. 4965, pp. 1–18, Springer, 2008.
 - 28 O. Dunkelman, D. Toz, *Analysis of two Attacks on Reduced-Round Versions of the SMS4*, proceedings of **ICICS 2008**, Lecture Notes in Computer Science vol. 5308, pp. 141–156, Springer, 2008.
 - 29 O. Dunkelman, N. Keller, *An Improved Impossible Differential Attack on MISTY1*, proceedings of **ASIACRYPT 2008**, Lecture Notes in Computer Science vol. 5350, pp. 441–454, Springer, 2008.
 - 30 O. Dunkelman, N. Keller, *A New Attack on the LEX Stream Cipher*, proceedings of **ASIACRYPT 2008**, Lecture Notes in Computer Science vol. 5350, pp. 539–556, Springer, 2008.
 - 31 J. Lu, O. Dunkelman, N. Keller, J. Kim, *New Impossible Differential Attacks on AES*, proceedings of **INDOCRYPT 2008**, Lecture Notes in Computer Science vol. 5365, pp. 279–293, Springer, 2008.
 - 32 O. Dunkelman, S. Indestege, N. Keller, *A Differential-Linear Attack on 12-Round Serpent*, proceedings of **INDOCRYPT 2008**, Lecture Notes in Computer Science vol. 5365, pp. 308–321, Springer, 2008.
 - 33 O. Dunkelman, N. Keller, *Cryptanalysis of CTC2*, proceedings of **CT-RSA 2009**, Lecture Notes in Computer Science vol. 5473, pp. 226–239, Springer, 2009.
 - 34 J.P. Aumasson, O. Dunkelman, F. Mendel, C. Rechberger, S.S. Thomsen, *Cryptanalysis of Vortex*, proceedings of **Africacrypt 2009**, Lecture Notes in Computer Science vol. 5580, pp. 14–28, Springer, 2009.
 - 35 C.d. Cannière, O. Dunkelman, M. Knezevic, *KATAN and KTANTAN — A Family of Small and Efficient Hardware-Oriented Block Ciphers*, proceedings of **Cryptographic Hardware and Embedded Systems 2009**, Lecture Notes in Computer Science vol. 5747, pp. 272–288, Springer, 2009.
 - 36 E. Andreeva, C. Bouillaguet, O. Dunkelman, J. Kelsey, *Herdling, Second Preimage and Trojan Message Attacks Beyond Merkle-Damgaard*, proceedings of **Selected Areas in Cryptography 2009**, Lecture Notes in Computer Science 5867, pp. 393–414, Springer, 2009.
 - 37 J.P. Aumasson, O. Dunkelman, S. Indestege, *Cryptanalysis of Dynamic SHA(2)*, proceedings of **Selected Areas in Cryptography 2009**, Lecture Notes in Computer Science 5867, pp. 415–432, Springer, 2009.
 - 38 O. Dunkelman, E. Fleischmann, M. Gorski, S. Lucks, *Related-Key Rectangle Attack of the Full 80-Round HAS-160 Encryption Mode*, proceedings of **INDOCRYPT 2009**, Lecture Notes in Computer Science 5922, pp. 157–168, Springer, 2009.
 - 39 C. Bouillaguet, O. Dunkelman, G. Leurent, P.-A. Fouque, *Another Look at Complementarity Properties*, proceedings of **Fast Software Encryption 2010**, Lecture Notes in Computer Science 6147, pp. 347–364, Springer, 2010.
 - 40 A. Biryukov, O. Dunkelman, N. Keller, D. Khovratovich, A. Shamir, *Key Recovery Attacks of Practical Complexity on AES-256 Variants With Up To 10 Rounds*, proceedings of **EUROCRYPT 2010**, Lecture Notes in Computer Science 6110, pp. 299–319, Springer, 2010.
 - 41 C. Bouillaguet, O. Dunkelman, G. Leurent, P.-A. Fouque, *Attacks on Hash Functions based on Generalized Feistel Application to Reduced-Round Lesamnta and SHAvite-3₅₁₂*, accepted to **Selected Areas in Cryptography 2010**, to appear in Lecture Notes in Computer Science, Springer.

-
- 42 O. Dunkelman, N. Keller, A. Shamir, *A Practical-Time Related-Key Attack on the KASUMI Cryptosystem Used in GSM and 3G Telephony*, proceedings of **CRYPTO 2010**, Lecture Notes in Computer Science 6223, pp. 393–410, Springer, 2010.
 - 43 O. Dunkelman, N. Keller, A. Shamir, *Improved Single-Key Attacks on 8-round AES-192 and AES-256*, proceedings of **ASIACRYPT 2010**, Lecture Notes in Computer Science vol. 6477, pp. 158–176, Springer, 2010.
 - 44 T. Ashur, O. Dunkelman, *Linear Analysis of Reduced-Round CubeHash*, accepted to Applied Cryptography and Network Security (ACNS) 2011, to appear in Lecture Notes in Computer Science.

REFEREED CONFERENCE (WITHOUT PROCEEDINGS)

- 1 O. Dunkelman, N. Keller, *Boomerang and Rectangle Attack on SC2000*, **NESSIE 2nd Workshop**, Egham, September 2001.
- 2 E. Biham, O. Dunkelman, *A Framework for Iterative Hash Functions — HAIFA*, **NIST's Hash Functions workshop 2006**, Santa Barbara, August 2006.
- 3 O. Dunkelman, B. Preneel, *Generalizing the Herding Attack to Concatenated Hashing Schemes*, **ECRYPT's hash function workshop 2007**, Barcelona, May 2007.
- 4 O. Dunkelman, N. Keller, *Treatment of the Initial Value in Time-Memory-Data Tradeoff Attacks on Stream Ciphers*, **State of the Art in Stream Ciphers 2008**, Lausanne, February 2008.

PUBLIC TECHNICAL REPORTS

- 1 O. Dunkelman, *An Analysis of Serpent-p and Serpent-p-ns*, presented at the rump session of AES 2nd conference, Rome 1999.
- 2 E. Biham, O. Dunkelman, V. Furman, T. Mor, *Preliminary report on the NESSIE submissions Anubis, Camellia, IDEA, Khazad, Misty1, Nimbus, Q*, NESSIE internal document NES/DOC/TEC/WP3/010/a.
- 3 O. Dunkelman, *Safety Margins for NESSIE submissions — Safer++ and Hierocrypt (L1/3)*, NESSIE internal document NES/DOC/TEC/WP3/015/a.
- 4 O. Dunkelman, *Comparing MISTY1 and KASUMI*, NESSIE internal document DOC/NES/TEC/WP5/029/a.
- 5 O. Dunkelman, N. Keller, *Linear Cryptanalysis of CTC*, IACR ePrint report 2006/250.
- 6 E. Biham, O. Dunkelman, *Differential Cryptanalysis in Stream Ciphers*, IACR ePrint report 2007/218.
- 7 E. Biham, O. Dunkelman, *A Framework for Iterative Hash Functions — HAIFA*, IACR ePrint report 2007/278.
- 8 E. Biham, O. Dunkelman, *The SHAvite-3 Hash Function, A SHA-3 candidate*, 2009.
- 9 O. Dunkelman, T. E. Bjørstad, *Practical Attacks on NESHA-256*, IACR ePrint report 2009/384.
- 10 J. Kim, S. Hong, B. Preneel, E. Biham, O. Dunkelman, N. Keller, *Related-Key Boomerang and Rectangle Attacks*, IACR ePrint report 2010/019.

Patents

- 1 Carmi D. Gressel, Gregory V. Bard, O. Dunkelman, Avi Hechet, Ran Granot, *A System and Method to Preclude Message Modification in Data Authentication Systems through Efficient Use of Feedback in Cryptographic Functions*, patent WO/2008/029406, publication date 13.3.08.

Professional Activities

Program Chair of:

- **Fast Software Encryption 2009**
- **Cryptographers' Track of RSA (CT-RSA) 2012**

General Chair of:

- **SASC (The State of the Art of Stream Ciphers) 2008**

An IACR member (2001–*present*),

Member of the Program Committees of:

Venues with Proceedings in **Lecture Notes in Computer Science**, Springer

- **CRYPTO**:
2007, 2008, 2011
- **EUROCRYPT**:
2008, 2011
- **ASIACRYPT**: 2005
- **ESORICS (European Symposium on Research in Computer Security)**: 2011
- **Fast Software Encryption (FSE)**:
2006, 2007, 2008, 2009 (**chair**), 2010
- **Selected Areas in Cryptography (SAC)**:
2006, 2007, 2008, 2009, 2010, 2011
- **INDOCRYPT**:
2005, 2006, 2009
- Cryptographers' Track of RSA (CT-RSA):
2008, 2010, 2011, 2012 (**chair**)
- Inscrypt (SKLOIS Conference on Information Security and Cryptology): 2006
- Information Security and Cryptology (ICISC): 2007
- Western European Workshop on Research in Cryptology (WEWoRC):
2009, 2011
- Africacrypt: 2010
- Applied Cryptography and Network Security (ACNS): 2010
- Latincrypt: 2010
- Financial Cryptography: 2011

Venues with Proceedings by the American Computing Machine society (ACM)

- **ACM's Computer and Communications Security (ACM CCS): 2011**

Venues with no formal proceedings

- NESSIE 2nd workshop, London, September 2001
- NESSIE 3rd workshop, Munich, November 2002
- ECRYPT STVL, Workshop on Symmetric Key Encryption, Aarhus, May 2005
- August Penguin 4, (Israel's Linux conference), Hertzelia, August 2005
- ECRYPT's hash function workshop 2007, Barcelona, May 2007
- SECRYPT 2007
- FutureTech 2010
- LightSec 2011
- ECRYPT's hash function workshop 2011, Talinn, May 2011

Reviewer for:

- **Journal of Cryptology**
- **Journal of ACM**
- **Physical Letters A**
- **IEEE Transactions on Information Theory**
- **Designs, Codes and Cryptography**
- **IEEE Transactions on Information, Forensics and Security**
- **IEEE Transactions on Computers**
- **IEEE Transactions on Circuits and Systems II**
- **Information Processing Letters**
- **Journal of Discrete Mathematics**
- Journal of Systems and Software
- Journal of Information Sciences

-
- IET Journal of Information Security
 - Advances of Mathematics in Communications
 - Journal of Computer Science and Technology
 - Journal of Circuits, Systems, and Computers
 - International Journal of Computer Mathematics
 - The Computer Journal
 - ETRI Journal
 - IEICE Transactions
 - **CRYPTO**:
2004, 2006, 2009, 2010
 - **EUROCRYPT**:
2003, 2006, 2007, 2010
 - **ASIACRYPT**:
2003, 2004, 2006, 2007, 2009
 - **Fast Software Encryption (FSE)**:
2002, 2004, 2005
 - **Theory of Cryptography Conference (TCC)**:
2010, 2011
 - Cryptographers' Track of RSA (CT-RSA):
2006, 2009
 - AFRICACRYPT:
2009, 2011
 - **Conference on Algorithms and Complexity (CIAC)**: 2003
 - **International Colloquium on Automata, Languages and Programming (ICALP)**: 2005
 - SKLOIS Conference on Information Security and Cryptology (CISC): 2005
 - International Conference on Information Security and Cryptology (ICISC): 2005
 - Security and Cryptography for Networks (SCN): 2006
 - International Conference on Security of Information and Networks (SIN): 2007
 - Conference on RFID Security-07 (2007)
 - Latin American Theoretical Informatics Symposium (LATIN): 2008
 - IEEE International Conference on Information Privacy, Security, Risk and Trust (PASSAT): 2009
 - International Conference on Cryptology And Network Security (CANS): 2009

Students

- Ph.D. students

Michel Gorski	Cryptanalysis and Design of Symmetric Primitives, at the Bauhaus-University Weimar, Germany. Co-advisor with Prof. Stefan Lucks.
---------------	--

- Master students

Gauthier Van Damme	Symmetrische versleuteling voor RFID-tags, at the Katholieke Universiteit Leuven, Belgium. (daily supervisor).
Uri Avraham	At the Technion, Israel. Co-advisor with Prof. Eli Biham.

- Erasmus students

Deniz Toz	Analysis of two attacks on Reduced-Round Version of the SMS4, at the Katholieke Universiteit Leuven (original university: Middle East Technical University).
-----------	--

Juries

- **Ph.D. students**

Sebastiaan Indesteege	Advisor: Prof. Bart Preneel, K.U. Leuven, May 2010.
Gaëtan Leurent	Advisor: Prof. Pierre-Alain Fouque, École normale supérieure, September 2010.

- **Master students**

Yaniv Shaked	Advisor: Prof. Avishai Wool, Tel Aviv University, June 2006.
--------------	--

Community Service

– IACR discussion forum administrator	2010– <i>present</i>
– Member of the Technion's Graduate Student Organization Board	2004
Representing the students of the Computer Science Dept. in the board of the GSO.	
– Manager of the Servers of the Farms at Technion's dormitories	2000–2006
Volunteering as the manager of dorms computer servers — vipe.technion.ac.il and ns.stud.technion.ac.il .	
– Organizer of the Technion's Linux Installation Parties	1999–2006
– Co-Founder of the Haifa Linux Club (Haifux)	1998– <i>present</i>
The club has been active for the last nine years, and is a meeting point for Linux users all around Israel. I am one of the lecturers giving lectures at the club's meetings, and I was one of the organizers of the "Welcome to Linux" lecture series.	
– Advisor in the Computer Farms at Technion's dormitories	1998–2000
A volunteer, and afterward a manager, of the computer farms in the Technion's dormitories. The job required maintaining the computers, helping users in the farms, teaching new volunteers and managing Linux and NT computers.	
– Advisor in the Computer Farms at Kalai High School	1994–1995
Installation of software and hardware components, tutoring other students and teachers on how to use the equipment, etc. I received the Givataim's award for excellence in community service for that activity.	

Languages

Hebrew (native), English (fluent), French (basic level), Spanish (basic level), and Arabic (basic reading level).