Curriculum Vitae
Orr Dunkelman

Updated: November 2015

Department of Computer Science
University of Haifa
Haifa 31905
Israel
Born: Israel, 2th of December, 1980
Citizenship: Israeli

Tel:+972-4-828-8447, +972-54-529-1912
Fax: +972-4-824-9331
Email: orrd@cs.haifa.ac.il
Web page: http://www.cs.haifa.ac.il/~orrd/
Family status: Married + 2

Research and Professional Experience

Department of Computer Science – UNIVERSITY OF HAIFA Feb. 2011–*present*
Associate professor.

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 researcher position.

Département d'Informatique – ÉCOLE NORMALE SUPÉRIEURE Apr. 2008–Sep. 2009
Post-doctoral researcher position.
– Part of the ECRYPT 2 research effort (Apr. 2008–Sep. 2009).

Dept. Elektrotechniek-ESAT SCD/COSIC – KATHOLIEKE UNIVERSITEIT LEUVEN Oct. 2006–Mar. 2008
Post-doctoral researcher 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

Design and cryptanalysis of symmetric key primitives.
Cryptanalytic methods and techniques.
Privacy in the digital world.
Computer security.

Education

TECHNION – ISRAEL INSTITUTE OF TECHNOLOGY Mar. 2000–Feb. 2006
Ph.D. in Computer Science.
Dissertation: Techniques for Cryptanalysis of Block Ciphers.
Studied in the direct program towards Ph.D., formal enrollment Feb. 2002.
Advisor: Prof. Eli Biham

TECHNION – ISRAEL INSTITUTE OF TECHNOLOGY Oct. 1997–Mar. 2000
B.A. in Computer Science.
Studied in the Technion's excellence program.
Graduated "Summa cum laude"

Teaching Experience

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

UNIVERSITY OF HAIFA:

G Introduction to Cryptography (203.4444):
- Winter 2015/16 (lecturer in charge)
- Winter 2014/15 (lecturer in charge)
- Winter 2013/14 (lecturer in charge)
- Winter 2012/13 (lecturer in charge)
- Spring 2011 (lecturer in charge)

G Computer and Network Security (203.4448):
- Winter 2015/16 (lecturer in charge)
- Winter 2014/15 (lecturer in charge)
- Winter 2013/14 (lecturer in charge)
- Winter 2012/13 (In conjuction with the Technion's course)
- Winter 2011/12 (lecturer in charge)

U Computer Networks (203.3210):
- Spring 2015 (lecturer in charge)
- Spring 2014 (lecturer in charge)
- Spring 2013 (lecturer in charge)

G Seminar in Block Cipher Cryptanalysis (203.4325):
- Spring 2013 (lecturer in charge)

U Seminar in Computer Security (203.3365):
- Spring 2015 (lecturer in charge)
- Spring 2014 (lecturer in charge)
- Winter 2012/3 (lecturer in charge)

U Discrete Mathematics (203.1850):
- Spring 2012 (lecturer in charge)

G Seminar in Cryptanalysis of Hash Functions (203.4485):
- Spring 2012 (lecturer in charge)

WEIZMANN INSTITUTE OF SCIENCE:

G Design and Analysis of Hash Functions:
- Winter 2010/11 (along with Prof. Shamir)

G Secret Key Cryptography and Cryptanalysis:
- Spring 2010 (along with Prof. Shamir)

TECHNION – ISRAEL INSTITUTE OF TECHNOLOGY:

G Advanced Topics in Computer Security (236602):
- Winter 2005/6 (lecturer in charge: Prof. Biham)

G Computer Security (236350):
- Winter 2013 (lecturer in charge: Dr. Bitan)

- Spring 2010 (lecturer in charge: Dr. Bitan)
- Spring 2006 (as 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

TECHNION – ISRAEL INSTITUTE OF TECHNOLOGY:

G Modern Cryptology (236506):
- 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)

G Advanced Topics in Cryptology:
- 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)

G Numerical Analysis 2 (236320):
- Spring 2003 (exercise checking, lecturer in charge: Prof. Sidi)
- Spring 2002 (exercise checking, lecturer in charge: Prof. Sidi)

G Computer Security (236350):
- 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.

(U stands for an undergraduate course, G stands for a graduate course)

Research Grants

1. *Transfer Learning/Domain Adaptation and Advance Behavioral Analysis in sparse data for Fraud Detection Applications*, joint research project with R. El-Yaniv, S. Manor, C. Crammer (all four of us PIs), 26,500 USD, 2012–2013.
2. *Secure Lightweight Cryptography*, G.I.F. grant 2082/2011, 22,000 EUR, 2013.
3. *Security Analysis of Cryptographic Hash Functions*, I.S.F. grant, 190,000 ILS/year for four years, 2012–2016. In addition, a one-time equipment grant of 1,560,000 ILS was granted.
4. *Privacy Enhancing Technologies for Biometric Data Usage and Storage*, joing research project with M. Osadchy and M. Naor (I am the PI), Israel's Ministry of Science and Technology grant 3-9774, 659,699 ILS for three years, 2012–2016.
5. *Biometric Key Generation*, joint research project with M. Osadchy, Israel's Department of Defense Research & Development (MAFAT), 75,000 ILS/year for two years, 2014–2016.
6. *Post-Quantum Cryptography for Long-Term Security*, EU research project headed by T. Lange (with 11 participating universities), 161,500 EUR for three years, 2015–2018.
7. *Improving Cyber Security using Realistic Synthetic Face Generation*, joint research project with S. Gibson, J. C. Hernandez-Castro, C. Solomon, M. Osadchy, 484,600 ILS for three years, 2015–2017.

8. *Title confidential at the request of the funding source*, joint research with N. Keller, 53,000 USD for a year, 2015.

(In joint grants, the amount reported is my share)

Honors and Awards

1. 2014, **Krill award**.
2. 2012, **Best Paper Award**, CRYPTO 2012.
3. 2012, **Best Paper Award**, Fast Software Encryption 2012.
4. 2010–2011, Clore Post-Doctoral Fellowship.
5. 2010, Distinguished Lecturer (Top 12%), Technion.
6. 2008–2009, France Telecom Chaire (for postdoctoral studies).
7. 2006–2007, Rothschild Post-Doctoral Fellowship.
8. 2006, Distinguished Lecturer (Top 15%), Technion.
9. 2003–2006, Clore Ph.D. Scholarship.
10. 2000, Excellence Scholarship, Technion.

Steering Committees

2008–2013, 2015	**Selected Areas in Cryptography** workshop board
2009–2012	**Fast Software Encryption** steering committee
2012–2014	**Cryptographers' Track of RSA (CT-RSA)** steering committee

Editorial Boards

2009–*present*	**International Journal of Applied Cryptography (IJACT)**
2010–*present*	**International Journal of Computer Mathematics (JCOM)**

Project Reviewer for

1. **US-Israel Bi-National Science Foundation**
2. **US National Science Foundation**
3. **Research Foundation Flanders (FWO)** (Belgium)
4. **Israel's Ministry of Science and Technology (MOST) National Cyber Program**

Invited Panelist

1. NIST Hash Function Workshop — "SHA-256: A Suitable Replacement for SHA-1?", Gaithersburg, MD, USA, 31/10/05
2. Haifa Law & Technology Center's workshop **Privacy Workshop: from Theory to Practice** — commentator on "S-M-L-XL Data: Big Data as a New Informational Privacy Paradigm", University of Haifa, 12/12/13

Invitation-Only Workshops (and talks given at them)

Dagstuhl Seminars:	
Symmetric Cryptography Seminar – 07021 (Jan. 2007)	*A Unified Approach for Related Key Attacks*
Symmetric Cryptography Seminar – 09031 (Jan. 2009)	*SHAvite-3 - A New and Secure Hash Function*
International View of the State-of-the-Art of Cryptography and Security and its Use in Practice – 11262 (Jun. 2011)	*A Somewhat Historic View of Lightweight Cryptography*
Symmetric Cryptography Seminar – 12031 (Jan. 2012)	1. *An IDEA to Consider* 2. *Multiple Results on Multiple Encryption*
Symmetric Cryptography Seminar – 14021 (Jan. 2014)	*Sweet16: YALWBC, But Slightly Different*
Other Events:	
Early Symmetric Crypto, Echternach, Luxembourg (Jan. 2008)	1. *Improved Meet-in-the-Middle Attacks on Reduced-Round DES* 2. *What is the Best Attack?*
Hash functions in cryptology: theory and practice, Lorentz Center, Leiden, The Netherlands (Jun. 2008)	*Re-Visiting HAIFA and why you should Visit too*
Early Symmetric Crypto, Remich, Luxembourg (Jan. 2010)	1. *Attacks of Practical Time Complexity on the A5/3 Underlying Block Cipher* 2. *Low Data Complexity Attacks on AES* 3. *And Now for Something Completely Impossible*
Early Symmetric Crypto, Mondorf-les-Bains, Luxembourg (Jan. 2013)	*New Directions in Dividing: Le Fabuleux Destin d'MISTY1 (The Case of MISTY1)*
International State of the Art in Cryptography — Security (May 2013)	Does Lightweight Cryptography Imply Slightsecurity?

Invited Talks

International Venues:

1. Hash Functions — Much Ado about Something — given at **Elliptic Curves Cryptography 2008**, Utrecht, The Netherlands, 23/9/08.
2. Key Recovery Attacks of Practical Complexity on AES Variants — given at **IWCNS 2009**, Taipei, Taiwan, 15/12/09.
3. The Hitchhiker's Guide to the SHA-3 Competition — given at **Latincrypt 2010**, Puebla, Mexico, 10/8/10.
4. From Multiple Encryption to Knapsacks Efficient Dissection of Composite Problems, given at **INDOCRYPT 2012**, Kolkata, India, 11/12/12.

Domestic Venues:

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. New Hash Functions Proposals — given at TaiWan Information Security Center (TWISC), Taipei, Taiwan, 17/11/08.
4. Hash Functions — As You Like It — given at TaiWan Information Security Center (TWISC),Taipei, Taiwan, 19/11/08.
5. The Not So Happily-Ever After End of AES' Security Fairytale — given at **CryptoDay 2010** at the Technion, Haifa, Israel, 9/6/10.

6 Privacy Preserving Biometric Database — given at Korea University, Seoul, South Korea, 9/12/11.
7 The Hitchhiker's Guide to the SHA-3 Competition — given at **Cryptoday 2012** at the Technion, Haifa, Israel, 4/7/12.
8 A Practical-Time Related-Key Attack on the KASUMI Cryptosystem Used in GSM and 3G Telephony — given at the "80th Anniversary of Broken the Enigma and Return to the Roots" at the Military University of Technology, Warsaw, Poland, 7/11/12.
9 Four Rounds are Not Enough — given at **Keccak & SHA-3 Day**, Université Libre de Bruxelles, Brussels, Belgium, 27/3/13.
10 Cyber Warfare from a Technological Point of View — given at **Technology, Law, and National Security in a Changing World**, University of Haifa, Israel, 29/10/13.
11 Finding Yourself Is The Key – Biometric Key Derivation that Keeps Your Privacy — given at **Haifa Security Research Seminar 2014** at IBM Haifa Research Labs, Haifa, Israel, 1/12/14.
12 Finding Yourself is the Key - Biometric Key Derivation Which Keeps Your Privacy — given at **Cyberday 2015** at the Technion, Haifa, Israel, 29/7/15.

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 How to Steal Cars – A Practical Attack on KeeLoq — given at Technion, Israel, 4/12/07.
11 Unified Related-Key Attacks — given at École Normale Supiérieure, France, 22/5/08.
12 Treatment of the Initial Value in Time-Memory-Data Tradeoff Attacks on Stream Ciphers — given at University of Rennes 1, France, 13/6/08.
13 Treatment of the Initial Value in Time-Memory-Data Tradeoff Attacks on Stream Ciphers — given at Katholieke Universiteit Leuven, Belgium, 7/7/08.
14 Hash Functions — Much Ado about Something — given at University of Wollongong, Australia, 5/12/08.
15 Treatment of the Initial Value in Time-Memory-Data Tradeoff Attacks on Stream Ciphers — given at Tel Aviv University, Israel, 8/2/09.
16 Traffic Analysis Attacks on a Continuously-Observable Steganographic File System — given at Tel Aviv University, Israel, 9/2/09.
17 Treatment of the Initial Value in Time-Memory-Data Tradeoff Attacks on Stream Ciphers — given at University of Haifa, Israel, 11/2/09.
18 Traffic Analysis Attacks on a Continuously-Observable Steganographic File System — given at Technion, Israel, 7/4/09.
19 KATAN & KTANTAN — A Family of Small and Efficient Hardware-Oriented Block Ciphers — given at Technical university of Graz, Austria, 8/5/09.
20 KATAN & KTANTAN — A Family of Small and Efficient Hardware-Oriented Block Ciphers — given at Katholieke Universiteit Leuven, Belgium, 14/9/09.
21 Key Recovery Attacks of Practical Complexity on AES Variants — given at École Normale Supiérieure, France, 17/9/09.

22 Key Recovery Attacks of Practical Complexity on AES Variants — given at University of Rennes 1, France, 25/9/09.
23 Key Recovery Attacks of Practical Complexity on AES Variants — given at Tel Aviv University, Israel, 29/11/09.
24 Key Recovery Attacks of Practical Complexity on AES Variants — given at Microsoft Research, Seattle, USA, 30/11/09.
25 Key Recovery Attacks of Practical Complexity on AES Variants — given at Technion, Israel, 24/12/09.
26 Key Recovery Attacks of Practical Complexity on AES Variants — given at Haifa University, Israel, 6/1/10.
27 Attacks of Practical Time Complexity on the A5/3 Underlying Block Cipher — given at Tel Aviv University, Israel, 7/1/10.
28 A Practical-Time Attack on the KASUMI Cryptosystem Used in GSM and 3G Telephony — given at Katholieke Universiteit Leuven, Belgium, 7/5/10.
29 A Practical-Time Attack on the KASUMI Cryptosystem Used in GSM and 3G Telephony — given at Ruhr-Universität, Bochum, Germany, 27/5/10.
30 A Practical-Time Related-Key Attack on the KASUMI Cryptosystem Used in GSM and 3G Telephony — given at École Normale Supiérieure, France, 8/7/10.
31 Improved Single-Key Attacks on 8-round AES, given at École Normale Supiérieure, France, 13/7/10.
32 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.
33 The Hitchhiker's Guide to the SHA-3 Competition — given at Microsoft Research, Seattle, USA, 3/9/10.
34 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.
35 Rethinking IDEA — given at École Normale Supiérieure, France, 4/7/11.
36 A Somewhat Historic View of Lightweight Cryptography — given at École Normale Supiérieure, France, 29/9/11.
37 Minimalism in Cryptography: The Even-Mansour Scheme Revisited — given at University of Haifa, Israel, 13/6/12.
38 Minimalism in Cryptography: The Even-Mansour Scheme Revisited — given at Tel Aviv University, Israel, 18/6/12.
39 History Repeats itself, also in Cryptography — given at Military Technology University, Warsaw, Poland, 6/11/12.
40 New Directions in Dividing: Le Fabuleux Destin d'MISTY1 (The Case of MISTY1) — given at Katholieke Universiteit Leuven, Belgium, 28/3/13.
41 Efficient Dissection of Bicomposite Problems, with Applications to Cryptanalysis, Knapsacks, and Combinatorial Search Problems — given at Tel Aviv University, Israel, 23/10/13.
42 Meet in the Middle Attacks — given at Centrum Wiskunde & Informatica (CWI), Amsterdam, The Netherlands, 18/2/14.
43 Meet in the Middle Attacks — The Next Generation — given at Centrum Wiskunde & Informatica (CWI), Amsterdam, The Netherlands, 18/2/14.
44 Does Lightweight Cryptography Imply Slightsecurity? — given at University of Kent, Canterbury, UK, 6/3/14.
45 When Cryptography is not the Answer (even when it is) — given at Technische Universität Darmstadt, Germany, 24/6/14.
46 When Cryptography is not the Answer (even when it is) — given at Ruhr-Universität, Bochum, Germany, 26/6/14.
47 When Cryptography is not the Answer (even when it is) — given at Technische Universität Berlin, Germany, 27/6/14.

48 How to Private ly Find Double Acquisitions in Biometric Databases — given at Weizmann Institute of Science (as part of the Greater Tel Aviv Cryptography Seminar), Rehovot, Israel, 5/2/15.

International Summer/Winter School/Special Courses

International Winter/Summer Schools:	
3rd ECRYPT Ph.D. Summer School, Advanced Topics in Cryptography, May 2008, Greece	*Related-Key Attacks*
ECRYPT II Summer School on Design and Security of Cryptographic Algorithms and Devices, May-Jun. 2011, Bulgaria	*Related-Key Attacks*
The São Paulo Advanced School of Cryptography, Oct. 2011, Brazil	1. *Advanced Techniques for the Cryptanalysis of Block Ciphers* 2. *Related-Key Attacks*
Summer School on Design and Security of Cryptographic Functions, Algorithms and Devices, Jun.-Jul. 2013, Bulgaria	1. *Multiple Encryption - New Cryptanalytic Algorithms and Applications* 2. *Combined Attacks - from Boomerangs to Sandwiches and Differential-Linear*
The 2nd TCE Summer School on Computer Security, Jul. 2013, Israel	*When Cryptography is not the Answer (even when it is)*
The 4th Bar-Ilan Winter School on Cryptology, Feb. 2014, Israel	1. *Generic Cryptanalytic Attacks* 2. *Related key attacks* 3. *The Advanced Encryption Standard (AES)*
Summer School on Design and security of cryptographic algorithms and devices for real-world applications, Jun. 2014, Croatia	*Combined Attacks — from Boomerangs to Sandwiches and Differential-Linear*
The 4th TCE Summer School on Computer Security, Sep. 2015, Israel	*TLS/SSL — (Mis)Protecting our Connections' Security*
International Courses:	
COSIC International Course, Jul. 2007, Belgium	*Block Ciphers and Stream Ciphers*

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 O. Dunkelman, editor of *Cryptographers' Track RSA 2012*, Lecture Notes in Computer Science vol. 7178, Springer, 2012, ISBN 978-3-642-27953-9.

3 E. Biham, O. Dunkelman, *Techniques for Cryptanalysis of Block Ciphers*, to appear in 2016, Springer.

4 O. Dunkelman, L. Keliher, editors of *Selected Areas in Cryptography 2015*, to appear in Lecture Notes in Computer Science in 2016, Springer.

JOURNAL PAPERS

1 O. Dunkelman, N. Keller, *A New Criterion for Nonlinearity of Block Ciphers*, **IEEE Transactions on Information Theory**, vol. 53, No. 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*, **Journal of Cryptology**, vol. 25, No. 1, pp. 136–157, Springer, 2012.

5 J. Kim, S. Hong, B. Preneel, E. Biham, O. Dunkelman, N. Keller, *Related-Key Boomerang and Rectangle Attacks: Theory and Experimental Analysis*, **IEEE Transactions on Information Theory**, vol. 58, No. 7, pp. 4948–4966, IEEE, 2012.

6 O. Dunkelman, N. Keller, *Cryptanalysis of the Stream Cipher LEX*, **Design, Codes, and Cryptography**, vol. 67, No. 3, pp. 357–373, 2013.

7 C. Bouillaguet, P. Derbez, O. Dunkelman, P.-A. Fouque, N. Keller, V. Rijmen, *Low Data Complexity Attacks on AES*, **IEEE Transactions on Information Theory**, vol. 58, No. 11, pp. 7002–7017, 2012.

8 I. Dinur, O. Dunkelman, A. Shamir, *Improved Practical Attacks on Round-Reduced Keccak*, **Journal of Cryptology**, vol. 27, No. 2, pp. 183–209, 2014.

9 O. Dunkelman, N. Keller, A. Shamir, *A Practical-Time Related-Key Attack on the KASUMI Cryptosystem Used in GSM and 3G Telephony*, **Journal of Cryptology**, vol. 27, No. 4, pp. 824–849, 2014.

10 I. Dinur, O. Dunkelman, N. Keller, A. Shamir, *Dissection: A New Paradigm for Solving Bicomposite Search Problems*, **Communications of ACM**, vol. 57, No. 10, pp. 98–105, 2014.

11 O. Dunkelman, N. Keller, A. Shamir, *Slidex Attacks on the Even-Mansour Encryption Scheme*, **Journal of Cryptology**, vol. 28, No. 1, pp. 1–28, 2015.

12 E. Biham, O. Dunkelman, N. Keller, A. Shamir, *New Attacks on IDEA with at Least 6 Rounds*, **Journal of Cryptology**, vol. 28, No. 2, pp. 209–239, 2015.

13 O. Dunkelman, N. Keller, A. Shamir, *Improved Single-Key Attacks on 8-round AES-192 and AES-256*, **Journal of Cryptology**, vol. 28, No. 3, pp. 397–422, 2015.

14 O. Dunkelman, N. Keller, A. Shamir, *Almost Universal Forgery Attacks on AES-Based MAC's*, **Design, Codes, and Cryptography**, vol. 76, No. 3, pp. 431–449.

15 O. Dunkelman, N. Keller, *Practical-Time Attacks Against Reduced Variants of MISTY1*, **Design, Codes, and Cryptography**, vol. 76, No. 3, pp. 601–627, 2015.

16 I. Dinur, O. Dunkelman, N. Keller, A. Shamir, *Reflections on slide with a twist attacks*, **Design, Codes, and Cryptography**, vol. 77, No. 2–3, pp. 633–651.

17 I. Dinur, O. Dunkelman, N. Keller, A. Shamir, *Key Recovery Attacks on Iterated Even-Mansour Encryption Schemes*, accepted to **Journal of Cryptology**.

18 E. Andreeva, C. Bouillaguet, O. Dunkelman, P.-A. Fouque, J. Hoch, J. Kelsey, A. Shamir, *New Second Preimage Attacks on Hash Functions*, accepted to **Journal of Cryptology**.

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. Indesteege, 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. Indesteege, 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. Canniére, 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, *Herding, 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. Indesteege, *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 Complementation 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-3$_{512}$*, proceedings of **Selected Areas in Cryptography 2010**, Lecture Notes in Computer Science 6544, pp. 18–35, Springer, 2011.

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*, proceedings of Applied Cryptography and Network Security (ACNS) 2011, Lecture Notes in Computer Science 6715, pp. 462–478, Springer, 2011.

45 C. Bouillaguet, O. Dunkelman, P.-A. Fouque, G. Leurent, *New Insights on Impossible Differential Cryptanalysis*, proceedings of **Selected Areas in Cryptography 2011**, Lecture Notes in Computer Science 7118, pp. 243–259, Springer, 2012.

46 I. Dinur, O. Dunkelman, A. Shamir, *Improved Attacks on Full GOST*, proceedings of **Fast Software Encryption 2012**, Lecture Notes in Computer Science 7549, pp. 9–28, Springer, 2012.

47 I. Dinur, O. Dunkelman, A. Shamir, *New attacks on Keccak-224 and Keccak-256* , proceedings of **Fast Software Encryption 2012**, in Lecture Notes in Computer Science 7549, pp. 442–461, Springer, 2012.

48 O. Dunkelman, N. Keller, A. Shamir, *Minimalism in Cryptography: The Even-Mansour Scheme Revisited*, proceedings of **EUROCRYPT 2012**, Lecture Notes in Computer Science 7237, pp. 336–354, Springer, 2012.

49 I. Dinur, O. Dunkelman, N. Keller, A. Shamir, *Efficient Dissection of Composite Problems, with Applications to Cryptanalysis, Knapsacks, and Combinatorial Search Problems*, proceedings of **CRYPTO 2012**, Lecture Notes in Computer Science 7417, pp. 719–740, Springer, 2012.

50 I. Dinur, O. Dunkelman, A. Shamir, *Collision Attacks on up to 5 Rounds of SHA-3 Using Generalized Internal Differentials*, proceedings of **Fast Software Encryption 2013**, Lecture Notes in Computer Science 8424, pp. 219–240, Springer, 2014.

51 T. Ashur, O. Dunkelman, *A Practical Related-Key Boomerang Attack for the Full MMB Block Cipher*, proceedings of **Cryptology and Network Security (CANS) 2013**, Lecture Notes in Computer Science 8257, pp. 271–290, Springer, 2013.

52 I. Dinur, O. Dunkelman, N. Keller, A. Shamir, *Key Recovery Attacks on 3-round Even-Mansour, 8-step LED-128, and Full AES*^{2}, proceedings of **ASIACRYPT 2013**, Lecture Notes in Computer Science 8269, pp. 337–356, Springer, 2013.

53 I. Dinur, O. Dunkelman, N. Keller, A. Shamir, *Improved Linear Sieving Techniques with Applications to Step-Reduced LED-64*, proceedings of **Fast Software Encryption 2014**, Lecture Notes in Computer Science 8540, pp. 390–410, Springer, 2014.

54 I. Dinur, O. Dunkelman, N. Keller, A. Shamir, *Cryptanalysis of Iterated Even-Mansour Schemes with Two Keys*, proceedings of **ASIACRYPT 2014**, Lecture Notes in Computer Science 8873, pp. 439–457, Springer, 2014.

55 A. Bar-On, I. Dinur, O. Dunkelman, V. Lallemand, N. Keller, B. Tsaban, *Cryptanalysis of SP Networks with Partial Non-Linear Layers*, proceedings of **EUROCRYPT 2015**, Lecture Notes in Computer Science 9056, pp. 315–342, Springer, 2015.

56 I. Dinur, O. Dunkelman, N. Keller, A. Shamir, *New Attacks on Feistel Structures with Improved Memory Complexities*, proceedings of **CRYPTO 2015**, Lecture Notes in Computer Science 9215, pp. 433–454, Springer, 2015.

57 I. Dinur, O. Dunkelman, M. Gutman, A. Shamir, *Improved Top-Down Techniques in Differential Cryptanalysis*, proceedings of **Latincrypt 2015**, Lecture Notes in Computer Science 9230, pp. 139–156, Springer, 2015.

REFEREED CONFERENCE POSTERS

1 T. Ashur, O. Dunkelman, *On the Anonymity of Israels General Elections*, proceedings of **CCS 2013**, pp. 1399–1402, ACM, 2013.

2 O. Dunkelman, M. Osadchy, M. Sharif, *POSTER: Secure Authentication from Facial Attributes with no Privacy Loss*, proceedings of **CCS 2013**, pp. 1403–1406, ACM, 2013.

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.
5 O. Dunkelman, D. Khovratovich, *Iterative Differentials, Symmetries, and Message Modification in BLAKE-256*, **ECRYPT II Hash Workshop 2011**, Tallinn, May 2011.

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.

PATENTS

1 Carmi D. Gressel, Gregory V. Bard, Orr 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:
1 **Fast Software Encryption 2009**
2 **Cryptographers' Track of RSA (CT-RSA) 2012**
3 **Selected Areas in Cryptography (SAC) 2015**

General Chair of:
1 **SASC (The State of the Art of Stream Ciphers) 2008**
2 University of Haifa's **Lightweight Crypto Day 2014**
3 **Taiwan-Israel Joint Workshop on Information Security 2014**
4 **Privacy Enhancing Technologies for Biometric Data** workshop, 2015
5 University of Haifa and Technion's **Lightweight Crypto Day 2015**
6 **Privacy Enhancing Technologies for Biometric Data** workshop, 2016

Organizer of the Following Summer Schools:
1 The 3rd TCE Summer School on Computer Security (2014, Technion, Israel)
2 The 5th TCE Summer School on Computer Security (2016, Technion, Israel)

— An IACR member (2001–*present*),
— An IEEE member (2015–*present*),

Member of the Program Committees of:

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

— **CRYPTO**: 2007, 2008, 2011, 2014, 2015

- **EUROCRYPT**: 2008, 2011, 2012
- **ASIACRYPT**: 2005, 2012, 2013, 2014
- **ESORICS (European Symposium on Research in Computer Security)**: 2011
- **Fast Software Encryption (FSE)**: 2006, 2007, 2008, 2009 (**chair**), 2010, 2013, 2014, 2015, 2016
- **Selected Areas in Cryptography (SAC)**: 2006, 2007, 2008, 2009, 2010, 2011, 2013, 2014, 2015 (**chair**)
- INDOCRYPT: 2005, 2006, 2009
- Cryptographers' Track of RSA (CT-RSA): 2008, 2010, 2011, 2012 (**chair**), 2014, 2015
- 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, 2012, 2016
- Applied Cryptography and Network Security (ACNS): 2010
- Latincrypt: 2010, 2012, 2014
- Financial Cryptography: 2011
- Australasian Conference on Information Security and Privacy (ACISP): 2013
- Cryptology and Network Security (CANS): 2013
- Mycrypt: 2016
- Privacy Enhancing Technologies: 2016

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

- **ACM's Computer and Communications Security (ACM CCS):** 2011, 2014
- **ACM's Symposium on Information, Computer, and Communications Security (AsiaCCS):** 2015

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, Tallinn, May 2011
- ECRYPT's lightweight cryptography workshop 2011, Louvain-La-Neuve, November 2011
- LightSec 2013

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 Cryptographic Engineering**
- 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
— Security and Communication Networks
— International Journal of Advanced Computer Technology
— Computer Standards & Interfaces
— IEICE Transactions
— **CRYPTO**: 2004, 2006, 2009, 2010
— **EUROCRYPT**: 2003,2006, 2007, 2010, 2013, 2015
— **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, 2013
— **International Colloquium on Automata, Languages and Programming (ICALP)**: 2005, 2013
— **Conference on Algorithms and Complexity (CIAC)**: 2003
— 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
— **Cryptographic Hardware and Embedded Systems (CHES)**: 2011
— 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.	2010

- Master students

Gauthier Van Damme	Symmetrische versleuteling voor RFID-tags, at the Katholieke Universiteit Leuven, Belgium. (daily supervisor).	2008
Uri Avraham	ABC — A New Framework for Block Ciphers at the Technion, Israel. Co-advisor with Prof. Eli Biham.	2012
Tomer Ashur	Security Assessment of Selected Cryptographic Symmetric-Key Primitives, At the University of Haifa, Israel.	2013

- 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).	2008

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.
Jianyong Huang	Advisor: , University of Wollongong, March 2013.
Tuomas Kortelainen	Advisor: Juha Kortelainen, University of Oulu, August 2014.
Yaniv Carmeli	Advisor: Prof. Eli Biham, Technion, November 2014.

- Master students

Yaniv Shaked	Advisor: Prof. Avishai Wool, Tel Aviv University, June 2006.
Idan Sheetrit	Advisor: Prof. Avishai Wool, Tel Aviv University, August 2011.
Andrey Yofis	Advisor: Prof. Martin C. Golumbic, University of Haifa, February 2012.
Mahmood Sharif	Advisor: Dr. Margarita Osadchy, University of Haifa, February 2014.
Inna Pollak	Advisor: Prof. Adi Shamir, Weizmann Institute of Science, April 2014.
Tsvi Cherny-Shahar	Advisor: Dr. David Movshovits, Interdisciplinary Center Hertzliya, April 2014.
Ofir Weisse	Advisors: Prof. Avishai Wool and Dr. Eran Tromer, Tel Aviv University, January 2015.

Community Service

– IACR discussion forum administrator 2010–*present*

– 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–*present*

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).