Curriculum Vitae: Professor Eli Biham

Updated: April 2013

Eli Biham

Office:	04-8294261	Computer Science Department, Dean
Cellular:	052-5552634	Technion – Israel Institute of Technology
		Haifa 32000
		Israel

Email: biham@cs.technion.ac.il

WWW: http://www.cs.technion.ac.il/∼biham/

Invited Professorships

October 1997	Invited Professor, Ecole Normale Supérieure, Paris, France
April-July 2004	Invited Professor, Ecole Normale Supérieure, Paris, France
December 2004–February 2005	Visiting Professorial Fellow, University of Wollongong, Australia

Research Interests

Cryptology, Cryptanalysis of symmetric primitives (block and stream ciphers and hash functions), Quantum cryptography and Quantum computation.

Awards

1. 2013, **IACR Distinguished Lecturer**, to be given in EUROCRYPT 2013, Greece, May 2013.
2. 2012, **IACR Fellow**.
3. 2012, **RSA Conference 2012 Award** for Excellence in the Field of Mathematics, for groundbreaking work on the cryptanalysis of symmetric-key ciphers.
4. 2004, The **Henry Taub prize** for excellence in research.
5. 2000, The Technion's **Muriel and David Jacknow award for excellence in teaching**.
6. 2000, The Technion's **Rei and Miriam Klein research award**.
7. 1998, United States of America, department of commerce, **Certificate of Appreciation**, for developing and submitting a candidate algorithm accepted for NIST's Advanced Encryption Standard development process.
8. 1993, The **Henry Taub prize** for excellence in research.
9. 1992, A reward received from Cryptech inc. for breaking the one-round variant of the REDOC-II cryptosystem. (the corresponding paper was presented at CRYPTO'91).
10. 1991, **The John F. Kennedy prize** for distinction in study from the Feinberg graduate school of the Weizmann Institute of Science.
11. 1990, A reward from **Xerox** corporation for breaking the hash function Snefru with two passes, received at the RUMP session of CRYPTO'90, 1990. (the corresponding paper was presented at CRYPTO'91).

Professional Activities

1993–2010 Member of the organizing/steering and program committees of the fast software encryption conference (FSE). Since 2002 the workshop is sponsored by the International Association for Cryptologic Research (IACR).

1998–2000 Vice chair of the computer science department curriculum committee.

1999–2004 **Director** of the International Association for Cryptologic Research (IACR). (elected position, two 3-year terms).

2000–2003 Chair of the computer science department curriculum committee.

2000–2001 Academic advisor for a course in *Information Systems Security* of the Technion's external studies department.

2002 Academic advisor for a course in *Information Systems Security* of the Technion's external studies department.

2001–2004 Member of the computing steering and development committee of the Technion.

2001 Member of the advisory committee for the Israeli Ministry of Justice on the regulations for the electronic signatures law.

2002–2007 **Associate Editor** of the Journal of Cryptology.

2002–2003 Acting head of the Technion's excellence program (for one semester: Spring 2002–2003; active participant in the program for many years).

2003 **Program chair** of EUROCRYPT 2003.

2003–ongoing Member of the governing council of the young persons' institute for the promotion of creativity and excellence (founded by Dr. Erika Landau).

2004–2006 Member of the strategic committee of the European project ECRYPT.

2005–2006 Member of the steering committees of SAC workshops.

2006–2008 Vice dean for gradute studies in the computer science department.

2005–ongoing Member of the Israel Standards Institute (ISI) standards committee 211402 – *Information Security: Digital Signatures.*

2008–ongoing **Dean** of the computer science department.

2012–ongoing Member of the external advisory committee (EAC) of the computer science department – school of computing of KAIST, South Korea.

2012 Chair of the Cyber grants and fellowships committee for the call for proposals of the ministry of science and the national cyber headquarters.

Memberships in Professional Associations

1990–ongoing Member of the International Association for Cryptologic Research (IACR).

Publications (Since 2008)

Refereed Papers in Professional Journals

J1. Elad Barkan, Eli Biham, Nathan Keller, *Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication*, **Journal of Cryptology**, Vol. 21, No. 3, pp. 392–429, 2008.

J2. Jongsung Kim, Seokhie Hong, Preneel B., Biham E., Dunkelman O., Keller N., *Related-Key Boomerang and Rectangle Attacks: Theory and Experimental Analysis* **IEEE Transactions on Information Theory**, Vol. 58, No. 7, pp. 4948–4966, 2012.

J3. Wim Aerts, Eli Biham, Dieter De Moitie, Elke De Mulder, Orr Dunkelman, Sebastiaan Indesteege, Nathan Keller, Bart Preneel, Guy A. E. Vandenbosch, Ingrid Verbauwhede, *A Practical Attack on KeeLoq*, **Journal of Cryptology**, Vol. 25, No. 1, pp. 136–157, 2012.

J4. Elad Barkan, Eli Biham, *In How Many Ways Can You Write Rijndael?*, **Journal of Cryptology**, to appear.

Books

B1. Eli Biham, Adi Shamir, *Differential Cryptanalysis of the Data Encryption Standard*, Springer Verlag, 192 pages, 1993.

B2. Eli Biham (Ed.), *Proceedings of Fast Software Encryption*, 4th international workshop, FSE'97, Haifa, Israel, January 1997, Lecture notes in computer science 1267, Springer Verlag, 1997.

B3. Eli Biham (Ed.), *Advances in cryptology — proceedings of EUROCRYPT 2003*, Warsaw, Poland, May 2003, Lecture notes in computer science 2656, Springer Verlag, 2003.

B4. B. Preneel, A. Biryukov, C. De Cannière, S. B. Örs, E. Oswald, B. Van Rompay, L. Granboulan, E. Dottax, G. Martinet, S. Murphy, A. Dent, R. Shipsey, C. Swart, J. White, M. Dichtl, S. Pyka, M. Schafheutle, P. Serf, E. Biham, E. Barkan, Y. Braziler, O. Dunkelman, V. Furman, D. Kenigsberg, J. Stolin, J-J. Quisquater, M. Ciet, F. Sica, H. Raddum, L. Knudsen, M. Parker, *Final Reports of European Project Number IST-1999-12324, named New European Schemes for Signatures, Integrity and Encryption (NESSIE)*, Springer Verlag, 2003, to appear.

B5. Eli Biham, Amr Youssef (Eds.), *Proceedings of SAC 2006*, Montreal, Canada, August 2006, Lecture notes in computer science 4356, Springer Verlag, 2007.

Book Sections

V1. The value "Differential Cryptanalysis" in *Encyclopedia of Information Security*, Kluwer, 2004.

V2. The value "Differential Cryptanalysis" in *Encyclopedia of Information Security, second edition*, Springer, 2011.

Patents

P1. Elad Barkan, Eli Biham, *Cryptanalysis Method and System*, Israel Patent #155671, Applied at 30/04/2003, Granted at 16/03/2005.

P2. Elad Barkan, Eli Biham, *Cryptoanalysis method and system*, US Patent #8009826, Issued on August 30, 2011.

P3. Elad Barkan, Eli Biham, *Cryptanalysis method and system*, US Patent #8295477, Issued on October 23, 2012.

Organization of Conferences

Conference Organizer

1997 Organizer and program chair of the fourth Fast Software Encryption workshop (**FSE**), Haifa, January 20–22, 1997.

2003 Program chair of **EUROCRYPT 2003**, Warsaw, Poland, May 4–8, 2003.

2006 Co-Chair of **SAC 2006**, Montreal, Canada, August 2006.

2007 Co-Organizer of Dagstuhl-Seminar in "Symmetric Cryptography", The international Conference and Research Center for Computer Science in Dagstuhl castle, Germany, January 2007.

Program/Organizing Committee Membership

1993 CRYPTO'93 conference, Santa Barbara, California, USA, August 22–26, 1993.

1993 Fast Software Encryption 1, Cambridge algorithms workshop in Cryptography, Cambridge, England, December 9–11, 1993.

1994 2nd ACM Conference on Computer and Communications Security, Fairfax, Virginia, USA, November 2–4, 1994.

1994 ASIACRYPT'94 conference, university of Wollongong, Australia, November 28–December 2, 1994.

1994 Fast Software Encryption 2, Leuven algorithms workshop in Cryptography, Leuven, Belgium, December 14–16, 1994.

1996 Fast Software Encryption 3, The Newton Institute, Cambridge, England, February 21–23, 1996.

1998 Fast Software Encryption 5, Ecole Normale Supérieure, Paris, France, March 1998.

1999 Fast Software Encryption 6, Rome, Italy, March 1999.

1999 EUROCRYPT'99, Prague, Czech republic, May 1999.

2000 Fast Software Encryption 7, New York, USA, April 2000.

2001 Fast Software Encryption 8, Yokohama, Japan, April 2001.

2002 Fast Software Encryption 9, Leuven, Belgium, February 2002.

2004 Fast Software Encryption 11, New-Delhi, India, February 2004.

2004 CRYPTO'04 conference, Santa Barbara, California, USA, August, 2004.

2005 Fast Software Encryption 12, Paris, France, February 2005.

2005 Krakow Hash Function workshop, Krakow, Poland, June 2005.

2006 RSA Conference 2006, Cryptographers' Track, February 13–17, 2006.

2006 EUROCRYPT'06 conference, May-June 2006.

2006 CRYPTO'06 conference, Santa Barbara, California, USA, August, 2006.

Workshops, Mini-Conferences and Summer Schools

2000 QUBIT 2000, Organized (together with Tal Mor) a one-day mini-conference on quantum information in the computer science department at the Technion, December 2000.

2003 QUBIT 2003, Organized (together with Tal Mor—chair, Martin Charles Golumbic, and Matty Katz) a one-day mini-conference on quantum information in the computer science department at the Technion, April 2003.

2008 Cryptoday 2008, May 2008.

2008 Electronic elections day (together with the office of the general accountant in the finance ministry), July 2008.

2009 Cryptoday 2009, July 2009.

2010 Cryptoday 2010, June 2010.

2011 Cryptoday 2011, June 2011.

2012 Cryptoday 2012, July 2012.

2012 TCE Summer School on Computer Security, with Eyal Kushilevitz, September 2012.

2013 Cyberday 2013, March 2013.

2013 TCE Summer School on Computer Security, with Yuval Ishai.