בס"ד

Nathan Keller – Curriculum Vitae

Born: Russia, 26.2.1982.
Citizenship: Israeli.
Family status: Married + 7.
Postal Address: Department of Mathematics, Bar Ilan University, Ramat Gan, Israel.
E-mail Address: nathan.keller@math.biu.ac.il
Webpage: www.ma.huji.ac.il/~nkeller

Research and Professional Experience

Bar Ilan University 2012-present

Senior Lecturer at the Department of Mathematics.

Weizmann Institute of Science 2009-2012

Koshland **Postdoctoral Fellow** at the Faculty of Mathematics and Computer Science.
Host: Prof. Elchanan Mossel.

Tel Aviv University 2009-present

Consultant at the Tsamir Institute for Mathematical Research.

Microsoft Research – Redmond 2006

Consultant at the Cryptography and Anti-Piracy Group.
Host: Dr. Ramarathnam Venkatesan.

Research Interests:

Combinatorics – Discrete harmonic analysis and its applications to Combinatorics and related fields.

Cryptography – Design and cryptanalysis of symmetric key cryptosystems.

Education:

Hebrew University of Jerusalem 2004-2009

Ph.D. degree in Mathematics.
Thesis title: Influences of variables on Boolean functions.

Advisor: Prof. Gil Kalai.

Technion – Israel Institute of Technology 1999-2002

M.Sc. degree in Mathematics *magna cum laude*.
Thesis title: Positivity of principal minors and sign symmetry.
Advisor: Prof. Daniel Hershkowitz.
Final grade: 97.2.

Technion – Israel Institute of Technology 1998-1999

B.A. degree in Mathematics *summa cum laude*.
Final grade: 94.5.

Teaching experience:

Bar Ilan University, Department of Mathematics 2012-present

Lecturer in the courses: Discrete Structures for Engineering students (2 times), Discrete Mathematics, Probabilistic Methods in Combinatorics, Introduction to Combinatorics, Linear Algebra II.

Hebrew University of Jerusalem, Institute of Mathematics 2004-2009

Teaching assistant in the courses: Set Theory (4 times), Ordinary Differential Equations, Advanced Topics in Calculus, Probabilistic Methods in Combinatorics.

Technion – Israel Institute of Technology, Faculty of Mathematics 1999-2000

Teaching assistant in the courses: Basic Calculus (2 times), Introduction to Probability Theory.

Honors, Awards and Grants:

Research Awards

Krill Prize 2014
(awarded by the Wolf Foundation)

Allon Fellowship 2013-2015
(awarded by the Israeli Higher Council for Education)

CRYPTO 2012 conference Best Paper Award 2012
(awarded by the International Association for Cryptographic Research)

Grants

Israel Science Foundation 2013-2017
(No. 402/13: "Influences of variables on Boolean functions")

Teaching Awards

Award for excellence in teaching 2009
(awarded by the Faculty of Exact Sciences of the Hebrew University)

Award for excellence in teaching 2005
(awarded by the Faculty of Exact Sciences of the Hebrew University)

Postdoctoral Fellowships

Koshland Postdoctoral Fellowship 2009-2012
(awarded by the Feinberg Graduate School of the Weizmann Institute of Science)

Graduate Studies

Adams Fellowship 2005-2009
(awarded by the Israeli Academy of Sciences and Humanities)

Orbach Prize for excellence in Ph.D. studies 2009
(awarded by the Institute of Mathematics of the Hebrew University)

Zuchovitsky Prize for excellence in Ph.D. studies 2007
(awarded by the Institute of Mathematics of the Hebrew University)

Faculty Award for excellence in M.Sc. studies 2002
(awarded by the Faculty of Mathematics of the Technion)

Undergraduate Studies

Excellence Program 1999
(awarded by the Technion, included full tuition and a stipend during
the B.A. studies, and special studying programs)

President List of Distinction for excellence in B.A. studies 1999
(awarded by the Technion, in both the Winter and the Spring semesters)

Mathematical Olympiads

Bronze Medal in the International Mathematical Olympiad (Taiwan) 1998

First Place in the Grossman Mathematics Olympiad 1998

First Place in the Gillis Mathematics Olympiad 1998

First Place in the "Championship of Shools" team Mathematics Olympiad 1998

Bronze Medal in the International Mathematical Olympiad (Argentina) 1997

First Place in the International Tournament of Towns 1997

Professional Activities:

Co-Organizer of the Combinatorics session at the American Mathematical Society – Israel Mathematical Union Meeting 2014

Co-Organizer of the "Lightweight Crypto Day" conference 2014

Indocrypt 2013 Conference – Program Committee Member 2013

Eurocrypt 2013 Conference – Program Committee Member 2013

Organizer of the Departmental Combinatorics Seminar at the Bar Ilan University 2012-present

Organizer of the Discrete Mathematics and Theoretical Computer Science session at the Israel Mathematical Union Meeting 2012

CT-RSA 2012 Conference – Program Committee Member 2011

Co-Organizer of the departmental Combinatorics Seminar at the Hebrew University 2007-2009

Fast Software Encryption 2009 conference - Program Committee Member 2008

Co-Organizer of a Matrix Theory weekly Seminar at the Technion 2002

International Tournament of Towns – Member of the grading committee 1999

Refereeing papers for numerous journals and conferences, including: 2004-present
Annals of Probability, SIAM Journal on Discrete Mathematics, SIAM Journal on Computing, Combinatorica, Israel Journal of Mathematics, Linear Algebra and its Applications, Electronic Journal of Linear Algebra, Groups Complexity and Cryptography, IEEE Transactions on Computers, IEEE Transactions on Information Theory, Theory of Computing, Design Codes and Cryptography, Information Processing Letters, Information Science, Security and Communication Networks, Physics Letters A, CRYPTO conference, Eurocrypt conference, Asiacrypt conference, FSE conference, SAC conference, CT-RSA conference, Indocrypt conference, ICALP conference, RANDOM conference.

Seminar and Conference Invited talks:

Mathematics Colloquium, Haifa University	March, 2014
"Lightweight Crypto Day" conference, Haifa University	February, 2014
Combinatorics Seminar, Hebrew University	December, 2013
Theoretical Computer Science Seminar, Hebrew University	November, 2013
Mathematics Colloquium, Holon Institute of Technology	Novermber, 2013
Special Cryptography Seminar, New York University	October, 2013
Security Seminar, Stanford University	October, 2013
Conference on "Functional inequalities in Discrete Spaces with applications", UC Berkeley	September, 2013
Combinatorics Seminar, Bar Ilan University	March, 2013
Analysis Seminar, Bar Ilan University	November, 2012
Crypto Day Conference, Technion	June, 2012
Theoretical Computer Science Seminar, Hebrew University	March, 2012
Probability Seminar, Bar Ilan University	March, 2012
Annual Meeting of the Israeli Mathematical Union, Discrete Mathematics Session, Bar Ilan University	June, 2011
Combinatorics seminar, Tel Aviv University	May, 2011
Mathematics Colloquium, Bar Ilan University	January, 2011
Combinatorics seminar, Technion	January, 2011
Winter Meeting of the Israel Mathematical Union, Tel Aviv University	December, 2010
Probability seminar, Bar Ilan University	December, 2010
Combinatorics seminar, Hebrew University	November, 2010
Combinatorics seminar, Bar Ilan University	June, 2010
Haifa Workshop on Interdisciplinary applications of Graphs, Combinatorics, and Algorithms, Haifa University	May, 2010
Probability seminar, Technion	May, 2010

Geometric Analysis and Probability Seminar, Weizmann Institute	May, 2010
Midrasha Mathematicae - Discrete Probability and Geometry Conference, Hebrew University	December, 2009
Special Cryptogtaphy seminar, Microsoft Research, Seattle	September, 2009
Oded Schramm Memorial Conference, Microsoft Research, Seattle (student poster)	August, 2009
Geometric Analysis and Probability Seminar, Weizmann Institute	June, 2009
Combinatorics seminar, Hebrew University	June, 2009
Student Probability Day, Weizmann Institute	May, 2009
Haifa Matrix Conference, Technion	May, 2009
Combinatorics seminar, Tel Aviv University	March, 2009
Combinatorics seminar, Technion	March, 2009
Special Guest Lecture Series, Security Group, NDS inc.	February, 2009
Combinatorics seminar, Bar Ilan University	January, 2009
Workshop on interactions between Probability Theory and Computer Science, Cornell University (student poster).	March, 2008
Special Cryptography seminar, Rutgers University	March, 2008
Combinatorics seminar, Hebrew University	March, 2008
Special Guest Lecture Series, Security Group, NDS inc.	February, 2008
Combinatorics seminar, Bar-Ilan University	January, 2008
Combinatorics seminar, Technion	November, 2007
Jerusalem Mathematics Colloquium – Zuchovitsky lecture	June, 2007
Random Structures and Algorithms Conference, Tel Aviv University	May, 2007
Student Probability Day, Weizmann Institute	March, 2007
Cryptography seminar, Technion	June, 2006
Cryptography and Complexity seminar, Weizmann Institute	May, 2006
Computer Science Theory seminar, Hebrew University	March, 2006

Eurocrypt Conference, Aarhus (Denmark) May, 2005

Haifa Matrix Conference, Technion January, 2005

Fast Software Encryption Conference, Lund (Sweden) February, 2003

Publications:

Published Papers in Combinatorics:

1) N. Keller, E. Mossel, and A. Sen, Geometric influences II: Correlation inequalities and noise sensitivity, *Annales de l'Institut Henri Poincare*, to appear.

2) N. Keller and G. Kindler, Quantitative relation between noise sensitivity and influences, *Combinatorica*, **33(1)** (2013), pp. 45-71.

3) N. Keller, A tight quantitative version of Arrow's impossibility theorem, *Journal of the European Mathematical Society*, **14(5)** (2012), pp. 1331-1355.

4) N. Keller, E. Mossel, and A. Sen, Geometric influences, *Annals of Probability*, **40(3)** (2012), pp. 1135-1166.

5) N. Keller, A simple reduction from a biased measure on the discrete cube to the uniform measure, *European Journal of Combinatorics*, **33(8)** (2012), pp. 1943-1957.

6) N. Keller, E. Mossel, and T. Schlank, A note on the entropy/influence conjecture, *Discrete Mathematics*, **312(22)** (2012), pp. 3364-3372.

7) E. Friedgut, G. Kalai, N. Keller, and N. Nisan, A quantitative version of the Gibbard-Satterthwaite theorem for three alternatives, *SIAM journal of Computing*, **40**(3) (2011), pp. 934-952.

8) N. Keller, On the influences of variables on Boolean functions in product spaces, *Combinatorics, Probability and Computing*, **20**(1) (2011), pp. 83-102.

9) N. Keller, On the probability of a rational outcome for generalized social welfare functions on three alternatives, *Journal of Combinatorial Theory Series A*, **117**(4) (2010), pp. 389-410.

10) N. Keller, On the correlation between monotone families in the average case, *Advances in Applied Mathematics*, **43**(1) (2009), pp. 31-45.

11) N. Keller and H. Pilpel, Linear transformations of monotone functions on the discrete cube, *Discrete Mathematics*, **309**(12) (2009), pp. 4210-4214.

Published Papers in Cryptography:

1) O. Dunkelman, N. Keller, and A. Shamir, Almost universal forgery attacks on AES-based MACs, *Design, Codes and Cryptography*, to appear.

2) O. Dunkelman and N. Keller, Practical-time attacks on reduced-round Misty1, *Design, Codes and Cryptography*, to appear.

3) I. Dinur, O. Dunkelman, N. Keller, and A. Shamir, Dissection: A new paradigm for solving bicomposite search problems, *Communications of the ACM*, to appear (Invited and accepted to the "Research Highlights" section).

4) O. Dunkelman, N. Keller, and A. Shamir, Slidex attacks on the Even-Mansour Cryptosystem, *Journal of Cryptology*, to appear.

5) O. Dunkelman, N. Keller, and A. Shamir, Improved single-key attacks on 8-round AES-192 and AES-256, *Journal of Cryptology*, to appear.

6) O. Dunkelman, N. Keller, and A. Shamir, New data-efficient attacks on reduced-round variants of IDEA, *Journal of Cryptology*, to appear.

7) O. Dunkelman, N. Keller, and A. Shamir, A practical-time related-key attack on the KASUMI cryptosystem used in GSM and 3G telephony, *Journal of Cryptology*, to appear.

8) O. Dunkelman and N. Keller, Cryptanalysis of the stream cipher LEX, *Design, Codes, and Cryptography*, **67(3)** (2013), pp. 357-373.

9) C. Bouillaguet, O. Dunkelman, P.A. Fouque, N. Keller, and V. Rijmen, Low data complexity attacks on AES, *IEEE Transactions on Information Theory*, **58(11)** (2012), pp. 7002-7017.

10) J. Kim, S. Hong, B. Preneel, E. Biham, O. Dunkelman, and N. Keller, Related-key boomerang and rectangle attacks: Theory and experimental verification, *IEEE Transactions on Information Theory*, **58(7)** (2012), pp. 4948-4966.

11) W. Aerts, E. Biham, D. de Moitie, E. de Mulder, O. Dunkelman, S. Indesteege, N. Keller, B. Preneel, G. Vandenbosch, and I. Verbauwhede, A practical attack on KeeLoq, *Journal of Cryptology*, **25(1)** (2012), pp. 136-157.

12) O. Dunkelman and N. Keller, The effects of the omission of last round's MixColumns on AES, *Information Processing Letters* **110** (2010), pp. 304-308.

13) N. Keller and S. D. Miller, Distinguishing attacks on stream ciphers based on arrays of pseudo-random words, *Information Processing Letters* **110** (2010), pp. 129-132.

14) E. Barkan, E. Biham, and N. Keller, Instant ciphertext-only cryptanalysis of GSM encrypted communication, *Journal of Cryptology* **21** (2008), no. 3, pp. 392-429.

15) O. Dunkelman and N. Keller, Treatment of the initial value in time-memory-data tradeoff attacks on stream ciphers, *Information Processing Letters* **107** (2008), pp. 133-137.

16) O. Dunkelman and N. Keller, A new criterion for nonlinearity of block ciphers, *IEEE Transactions on Information Theory* **53** (2007), no. 11, pp. 3944-3957.

Published Papers in Matrix Theory:

1) D. Hershkowitz and N. Keller, Spectral Properties of Sign Symmetric Matrices, *Electronic Journal of Linear Algebra* **13** (2005), pp. 90-110.

2) D. Hershkowitz and N. Keller, Positivity of Principal Minors, Sign Symmetry and Stability, *Linear Algebra and its Applications* **364** (2003), pp. 105-124.

Preprints in Cryptography:

1) I. Dinur, O. Dunkelman, N. Keller, and A. Shamir, Efficient dissection of composite problems, with applications to Cryptanalysis, Knapsacks and Combinatorial search problems, submitted to *Journal of the ACM.*

Conference Papers in Cryptography:

The papers below were presented in peer reviewed conferences in Cryptography and published in the series "Lecture Notes of Computer Science" (LNCS) of Springer-Verlag.

1) I. Dinur, O. Dunkelman, N. Keller, and A. Shamir, Improved linear sieving techniques, with applications to step-reduced LED-64, FSE 2014, to appear.

2) I. Dinur, O. Dunkelman, N. Keller, and A. Shamir, Key-recovery attacks on 3-round Even-Mansour, 8-step LED-128, and full AES^2, Asiacrypt 2013, to appear. (**Solicited for publication in Journal of Cryptology as one of the three best papers**).

3) I. Dinur, O. Dunkelman, N. Keller, and A. Shamir, Efficient dissection of composite problems, with applications to Cryptanalysis, Knapsacks and Combinatorial search problems, Crypto 2012, LNCS 7417, pp. 719-740. (**Best Paper Award**).

4) O. Dunkelman, N. Keller, and A. Shamir, Minimalism in cryptography: the Even-Mansour cryptosystem revisited, Eurocrypt 2012, LNCS 7237, pp. 336-354.

5) O. Dunkelman, N. Keller, and A. Shamir, Improved single key attacks on 8-round AES-192 and AES-256, Asiacrypt 2010, LNCS 6477, pp. 158-176. (**Solicited for publication in Journal of Cryptology as one of the three best papers**).

6) O. Dunkelman, N. Keller, and A. Shamir, A practical-time attack on the KASUMI cryptosystem used in GSM and 3G telephony, Crypto 2010, LNCS 6223, pp. 393-410.

7) A. Biryukov, O. Dunkelman, N. Keller, D. Khovratovich, and A. Shamir, Key recovery attacks of practical complexity on AES-256 variants with up to 10 rounds, Eurocrypt 2010, LNCS 6110, pp. 299-319.

8) O. Dunkelman and N. Keller, Cryptanalysis of CTC2, CT-RSA 2009, LNCS 5473, pp. 226-239.

9) O. Dunkelman and N. Keller, An improved impossible differential attack on Misty1, Asiacrypt 2008, LNCS 5350, pp. 441-454.

10) O. Dunkelman and N. Keller, A new attack on the LEX stream cipher, Asiacrypt 2008, LNCS 5350, pp. 539-556.

11) J. Lu, O. Dunkelman, N. Keller, and J. Kim, New impossible differential attacks on AES, Indocrypt 2008, LNCS 5365, pp. 279-293.

12) O. Dunkelman, S. Indesteege, and N. Keller, A differential-linear attack on 12-round Serpent, Indocrypt 2008, LNCS 5365, pp. 308-321.

13) S. Indesteege, N. Keller, O. Dunkelman, E. Biham, and B. Preneel, A practical attack on KeeLoq, Eurocrypt 2008, LNCS 4965, pp. 1-18.

14) E. Biham, O. Dunkelman, and N. Keller, A unified approach to related key attacks, FSE 2008, LNCS 5086, pp. 73-96.

15) J. Lu, J. Kim, N. Keller, and O. Dunkelman, Improving the efficiency of impossible differential cryptanalysis of reduced Camellia and Misty1, CT-RSA 2008, LNCS 4964, pp. 370-386.

16) G. Wang, N. Keller, and O. Dunkelman, The delicate issues of addition with respect to XOR differences, SAC 2007, LNCS 4876, pp. 212-231.

17) N.Keller, S. Miller, I. Mironov, and R. Venkatesan, MV3: A new stream cipher based on random walks and revolving buffers, CT-RSA 2007, LNCS 4377, pp. 1-19.

18) E. Biham, O. Dunkelman, and N. Keller, Improved Slide Attacks, FSE 2007, LNCS 4593, pp. 153-166.

19) E. Biham, O. Dunkelman, and N. Keller, A New Attack on 6-Round IDEA, FSE 2007, LNCS 4593, pp. 211-224.

20) E. Biham, O. Dunkelman, and N. Keller, A Simple Related-Key Attack on the Full SHACAL-1, CT-RSA 2007, LNCS 4377, pp. 20-30.

21) E. Biham, O. Dunkelman, and N. Keller, New Cryptanalytic Results on IDEA, Asiacrypt 2006, LNCS 4284, pp. 412-427.

22) J. Lu, J. Kim, N. Keller, and O. Dunkelman, Differential and Rectangle Attacks on Reduced-Round SHACAL-1, Indocrypt 2006, LNCS 4329, pp. 17-31.

23) O. Dunkelman, N. Keller, and J. Kim, Related-Key Rectangle Attack on the Full SHACAL-1, SAC 2006, LNCS 4356, pp. 28-44.

24) J. Lu, J. Kim, N. Keller, and O. Dunkelman, Related-Key Rectangle Attack on 42-Round SHACAL-2, ISC 2006, LNCS 4176, pp. 85-100.

25) E. Biham, O. Dunkelman and N. Keller, Related-Key Impossible Differential Attacks on 8-round AES-192, CT-RSA 2006, LNCS 3860, pp. 21-33.

26) O. Dunkelman and N. Keller, A New Criterion for Nonlinearity of Block Ciphers, CT-RSA 2006, LNCS 3860, pp. 295-312.

27) E. Biham, O. Dunkelman and N. Keller, Related-Key Rectangle Attack on the Full KASUMI, Asiacrypt 2005, LNCS 3788, pp. 443-461.

28) E. Biham, O. Dunkelman, and N. Keller, Related-Key Boomerang and Rectangle Attacks, Eurocrypt 2005, LNCS 3494, pp. 507-525.

29) E. Biham, O. Dunkelman, and N. Keller, New Combined Attacks on Block Ciphers, FSE 2005, LNCS 3557, pp. 126-144.

30) E. Barkan, E. Biham, and N. Keller: Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication, Crypto 2003, LNCS 2729, pp. 600-616.

31) E. Biham, O. Dunkelman, and N. Keller: Rectangle Attacks on 49-Round SHACAL-1, FSE 2003, LNCS 2883, pp. 22-35.

32) E. Biham, O. Dunkelman, and N. Keller, Differential-Linear Cryptanalysis of Serpent, FSE 2003, LNCS 2883, pp. 9-21.

33) E. Biham, O. Dunkelman, and N. Keller, Enhancing Differential-Linear Cryptanalysis, Asiacrypt 2002, LNCS 2501, pp. 254-266.

34) E. Biham, O. Dunkelman and N. Keller, New Results on Boomerang and Rectangle Attacks, FSE 2002, LNCS 2365, pp. 1-16.

35) E. Biham, O. Dunkelman and N. Keller, The Rectangle Attack – Rectangling the Serpent, Eurocrypt 2001, LNCS 2045, pp. 340-357.

36) E. Biham, O. Dunkelman and N. Keller, Linear Cryptanalysis of Reduced-Round Serpent, FSE 2001, LNCS 2355, pp. 16-27.