בס"ד

Nathan Keller – Curriculum Vitae

Born: Russia, 26.2.1982.
Citizenship: Israeli.
Family status: Married + 11.
Postal Address: Department of Mathematics, Bar Ilan University, Ramat Gan, Israel.
E-mail Address: Nathan.Keller@biu.ac.il
Webpage: www.u.cs.biu/~nkeller

Research and Professional Experience

Bar Ilan University 2019-present

Professor, Department of Mathematics.

Bar Ilan University 2015-2019

Associate Professor, Department of Mathematics.

Bar Ilan University 2012-2015

Senior Lecturer, Department of Mathematics.

Weizmann Institute of Science 2009-2012

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

Tel Aviv University 2009-2018

Consultant, Tsamir Institute for Mathematical Research.

Microsoft Research – Redmond 2006

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

Research Interests:

Combinatorics – Discrete Fourier 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: Algebraic Structures for Engineering students (8 times), Discrete Mathematics, Discrete Mathematics for Engineering students (2 times), Probabilistic Methods in Combinatorics (5 times), Introduction to Combinatorics (8 times), Linear Algebra II, Cryptanalysis of symmetric key cryptosystems (7 times), Expander graphs and their applications (2 times), Analysis of Boolean functions (3 times), Graduate seminar (3 times).

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

Delbert Ray Fulkerson Prize (awarded by the American Mathematical Society (AMS) and the Mathematical Optimization Society (MOS)	2024
Rector's prize for scientific innovation (awarded by the Bar Ilan University)	2021
Elected Member, Israel Young Academy	2020
Erdős Prize (awarded by the Israel Mathematical Union)	2020
Rector's prize for scientific innovation (awarded by the Bar Ilan University)	2016
Krill Prize (awarded by the Wolf Foundation)	2014
Alon Fellowship (awarded by the Israeli Higher Council for Education)	2013-2015
CRYPTO 2012 conference Best Paper Award (awarded by the International Association for Cryptographic Research)	2012

Grants

Israel Science Foundation (No. 2669/21: "Fourier-analytic techniques in extremal combinatorics and beyond", with G. Kalai (Hebrew University))	2021-2025
European Research Council (ERC) Starting Grant (No. 757731 (LightCrypt): "New directions in lightweight cryptanalysis")	2017-2023
Israel Science Foundation (No. 1612/17: "Algebraic and analytic methods in extremal combinatorics", with G. Kalai (Hebrew University))	2017-2021
Binational US-Israel Science Foundation (No. 2014290: "Fourier analysis, influences, threshold phenomena, correlation inequalities, and Chvatal's conjecture", with J. Kahn (Rutgers) and G. Kalai (Hebrew University))	2015-2019
Samsung SDS Company (Whitebox cryptography)	2014-2016
Bar Ilan University Internal Grant (Combinatorics and Cryptography)	2015

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

Teaching Awards

Outstanding Lecturer Award 2020
(awarded by the Vice Rector of the Bar Ilan University)

Outstanding Lecturer Award 2015
(awarded by the Vice Rector of the Bar Ilan University)

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-Founder and Director of the Excellence Program for M.Sc. Students, Mathematics Department, Bar Ilan University	2017-present
Co-Organizer of the Departmental Combinatorics Seminar at the Bar Ilan University	2012-present
Reviewer – Azrieli Postdoctoral Fellowships	2020-present
Organizer of the Israel Mathematical Union Student Talks Day	2024
Member, Israel Young Academy Member Selection committee	2021-2023
Member, Israel Academy of Sciences of Humanities (IASH) Committee for Foreign Postdoctoral Fellowships	2020-2023
Organizer of the Israel Mathematical Union Student Talks Day	2023
Crypto 2023 conference – Program Committee Member	2023
Head of the Academic Program for young students in Mathematics at the Bar Ilan University	2018-2022
Organizer of the Israel Mathematical Union Student Talks Day	2022
Organizer of the workshop: "New directions in Cryptanalysis of the AES"	2022
Co-Organizer of the workshop: "Reflections: A workshop honoring Ron Adin's and Yuval Roichman's 60'th birthday"	2022
Co-Organizer of the workshop: "Integration of Charedi students in regular Programs in universities"	2022
FSE 2022 conference – Program Committee Member	2021
Member of the Steering Committee of the Center for Advanced	2017-2020

Studies at the Mathematics Department, Bar Ilan University

Co-Organizer of the workshop: "See and be seen" for Post-doctoral students in the exact sciences	2020
FSE 2021 conference – Program Committee Member	2020
Annual meeting of the Israeli Mathematical Union 2020 – Organizing Committee Member	2020
Co-Organizer of the workshop: "Fractals and Dynamics: A workshop Honoring Boris Solomyak's 60'th birthday"	2020
Organizer of the Analysis of Boolean functions Seminar at the Bar Ilan University	2016-2019
Eurocrypt 2020 conference – Program Committee Member	2019
FPSAC 2020 conference – Organizing Committee Member	2019
Co-Organizer of the workshop "Student Combinatorics Day II", Bar Ilan University	2019
Co-Organizer of the workshop: "Research Retreat on NIST lightweight Candidates", Bar Ilan University	2019
Co-Organizer of the "Lightweight Crypto Day V" conference, Bar Ilan University	2019
FSE 2019 Conference - Program Committee Member	2018
Co-Organizer of the workshop "Student Combinatorics Day I", Bar Ilan University	2018
Co-Organizer of the "Lightweight Crypto Day IV" conference, Tel Aviv	2018
Co-Organizer of the conference: "The challenges of lightweight cryptanalysis", Bar Ilan University	2018
CSCML 2018 Conference - Program Committee Member	2018
Eurocrypt 2018 Conference – Program Committee Member	2018
FSE 2018 Conference - Program Committee Member	2018
Director of the Academic Program for talented young students in Mathematics at the Bar Ilan University	2014-2018
Co-Organizer of the Discrete Mathematics	2017

and Theoretical Computer Science session at the Israel Mathematical Union Meeting

Eurocrypt 2017 Conference – Program Committee Member 2017

SAC 2016 Conference – Program Committee Member 2016

Indocrypt 2016 Conference – Program Committee Member 2016

Co-Organizer of the "Lightweight Crypto Day III" conference, Technion 2016

CT-RSA 2016 Conference – Program Committee Member 2016

Asiacrypt 2015 Conference – Program Committee Member 2015

Co-Organizer of the "Lightweight Crypto Day II" conference, Technion 2015

SAC 2015 Conference – Program Committee Member 2015

Co-Organizer of the "Lightweight Crypto Day I" conference, Haifa University 2014

Indocrypt 2013 Conference – Program Committee Member 2013

Eurocrypt 2013 Conference – Program Committee Member 2013

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

FSE 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

Journal of the AMS, Inventiones Mathematicae, Journal of the EMS, Journal of the LMS, Annals of Probability, Probability Theory and Related Fields, Electronic Journal on Probability, Discrete Analysis, SIAM Journal on Computing, Bulletin of the AMS, SIAM Journal on Discrete Mathematics, Combinatorica, Journal of Combinatorial Theory: Series A, Journal of Combinatorial Theory: Series B, European Journal of Combinatorics, Israel Journal of Mathematics, Discrete and Computational Geometry, Linear Algebra and its Applications, Electronic Journal of Linear Algebra, Groups Complexity and Cryptography, Journal of Cryptology, 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, Theory of Computing Systems, Physics Letters A, CRYPTO conference, Eurocrypt conference, Asiacrypt conference, FSE conference, SAC conference, CT-RSA conference, Indocrypt conference, ICALP conference, RANDOM conference, SoCG conference.

Refereeing of grant proposals 2015-present

European Research Council (ERC Advanced Grant), Israel Science Foundation, Binational US-Israel Science Foundation, UK Royal Society, Research Foundation Flanders.

Current Student/Postdoc Supervision:

1. Eran Lambooij (Post-Doc)
2. Omri Marcus (M.Sc)
3. Ohad Sheinfled (M.Sc)
4. Asaf Rosemarin (M.Sc)
5. David Ross (M.Sc)
6. Nitay Reiter (M.Sc)

Past Student/Postdoc Supervision:

1. Rani Hod – Post Doctoral fellow, 2016-2019.
2. Ariel Weizmann – Ph.D., 2023. (Joint with Prof. Orr Dunkelman)
3. Ohad Klein – Ph.D., 2022.
4. Achiya Bar On – Ph.D., 2019.
5. Yuval Becker – M.Sc., 2020. (Joint with Prof. Boaz Tsaban)
6. Aviya Vaidberg – M.Sc., 2018.
7. Ariel Weizmann – M.Sc., 2018. (Joint with Prof. Orr Dunkelman)
8. Ohad Klein – M.Sc. with highest distinction, 2018.
9. Noam Lifshitz – M.Sc. with highest distinction, 2017.

10. Achiya Bar On - M.Sc. with highest distinction, 2016. (Joint with Prof. Boaz Tsaban)

Seminar and Conference Invited talks:

Workshop in memory of Prof. Avraham Trachtman, BIU	September, 2024
ISMP conference, Montreal, Canada	July, 2024
Mathematics Colloquium, University of Haifa	March, 2024
Combinatorics Seminar, Hebrew University	May, 2023
Computer Science Colloquium, Ben Gurion University	April, 2023
Mathematics Colloquium, Ben Gurion University	May, 2022
Mathematics Colloquium, Bar Ilan University	May, 2022
Mathematics Colloquium, Tel Aviv University	June, 2021
STOC Conference (talk given online)	June, 2021
Computer Science Colloquium, Hebrew University	May, 2021
UCLA-Caltech analysis seminar (talk given online)	April, 2021
Mathematics Colloquium, Haifa University (talk given online)	January, 2021
Jerusalem Mathematics Colloquium, Hebrew University (talk given online)	December, 2020
Erdős Prize Talk, Annual Meeting of the Israel Mathematical Union (talk given online)	September, 2020
Combinatorics Seminar, Hebrew University (talk given online)	June, 2020
Eurocrypt Conference (talk given online)	May, 2020
Simons Collaboration on Algorithms and Geometry Monthly Meeting, New York	February, 2020
Discrete Mathematics Seminar, Princeton	February, 2020
ERC Mini-workshop: Extremal Problems in Combinatorial Geometry, Eilat	February, 2020
Probability Seminar, Bar Ilan University	January, 2020
Combinatorics Seminar, Tel Aviv University	November, 2019

Annual Meeting of the Israel Mathematical Union, Mathematical Education Session	June, 2019
Theoretical Computer Science Seminar, Weizmann Institute	May, 2019
"Lightweight Crypto Day" conference, Bar Ilan University	March, 2019
Combinatorics Seminar, Tel Aviv University	December, 2018
Jerusalem Mathematics Colloquium, Hebrew University	November, 2018
Probability Seminar, Technion	November, 2018
Workshop on "The challenges of lightweight cryptanalysis", Bar Ilan University	April, 2018
Mathematics Colloquium, Bar Ilan University	April, 2018
Theoretical Computer Science Seminar, Technion	January, 2018
GTACS Seminar, Bar Ilan University	November, 2017
Cryptology Seminar, KU Leuven (Belgium)	June, 2017
Theoretical Computer Science Seminar, Tel Aviv University	March, 2017
Combinatorics Seminar, Bar Ilan University	November, 2016
Cryptology Seminar, KU Leuven (Belgium)	May, 2016
Geometric Analysis and Probability Seminar, Weizmann Institute	February, 2016
Combinatorics Seminar, Hebrew University	January, 2016
Combinatorics Seminar, Bar Ilan University	October, 2015
GTACS Seminar, Bar Ilan University	May, 2015
Combinatorics Seminar, Bar Ilan University	June, 2014
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	November, 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 Journal Papers in Combinatorics:

1) N. Keller, N. Lifshitz, and O. Sheinfeld, Improved covering results for conjugacy classes of symmetric groups via hypercontractivity, *Forum Mathematics, Sigma*, to appear.

2) D. Ellis, N. Keller, and N. Lifshitz, Stability for the Complete Intersection Theorem, and the Forbidden Intersection Problem of Erdős and Sós, *Journal of the European Mathematical Society*, **26(5)** (2024), pp. 1611-1654.

3) N. Keller, N. Lifshitz, D. Minzer, and O. Sheinfeld, On t-intersecting families of permutations, *Advances in Mathematics,* **445** (2024), 109650, pp. 1-28.

4) N. Keller and O. Klein, Proof of Tomaszewski's conjecture on randomly signed sums, *Advances in Mathematics,* **407** (2022), 108558, pp. 1-39.

5) N. Keller and N. Lifshitz, The junta method for hypergraphs and the Erdős-Chvátal simplex conjecture, *Advances in Mathematics,* **392** (2021), 107991, pp. 1-95.

6) N. Keller and O. Klein, A structure theorem for almost low-degree functions on the slice, *Israel Journal of Mathematics,* **240** (2020), pp. 179-221.

7) N. Keller and O. Klein, Biased halfspaces, noise sensitivity, and local Chernoff inequalities, *Discrete Analysis,* **2019:13**, pp. 1-50.

8) D. Ellis, N. Keller, and N. Lifshitz, Stability versions of Erdos-Ko-Rado type theorems, via isoperimetry, *Journal of the European Mathematical Society*, **21(12)** (2019), pp. 3857-3902.

9) N. Keller and N. Lifshitz, A note on large H-intersecting families, *SIAM Journal on Discrete Mathematics*, **33(1)** (2019), pp. 398-401.

10) D. Ellis, N. Keller, and N. Lifshitz, On a biased edge isoperimetric inequality for the discrete cube, *Journal of Combinatorial Theory, Series A*, **163** (2019), pp. 118-162.

11) N. Keller and N. Lifshitz, Approximation of biased Boolean functions of small total influence by DNF's, *Bulletin of the London Mathematical Society,* **50(4)** (2018), pp. 667-679.

12) D. Ellis, N. Keller, and N. Lifshitz, On the structure of subsets of the discrete cube with small edge boundary, *Discrete Analysis*, **2018:9**, pp.1-29.

13) E. Friedgut, J. Kahn, G. Kalai, and N. Keller, Chvatal's conjecture and correlation inequalities, *Journal of Combinatorial Theory, Series A*, **156** (2018), pp. 22-43.

14) G. Kalai, N. Keller, and E. Mossel, On the correlation of increasing families, *Journal of Combinatorial Theory, Series A*, **144** (2016), pp. 250-276.

15) I. Benjamini, D. Ellis, E. Friedgut, N. Keller, and A. Sen, Juntas in the ell_1-grid and Lipschitz maps between discrete tori, *Random Structures and Algorithms* **49(2)** (2016), pp. 253-279.

16) Y. Filmus, H. Hatami, N. Keller, and N. Lifshitz, Bounds on the sum of L1 influences, *Israel Journal of Mathematics*, **214(1)** (2016), pp. 167-192.

17) N. Keller, E. Mossel, and A. Sen, Geometric influences II: Correlation inequalities and noise sensitivity, *Annales de l'Institut Henri Poincare*, **50(4)** (2014), pp. 1121–1139.

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

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

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

21) 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.

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

23) 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.

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

25) 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.

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

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

Published Journal Papers in Cryptography:

1) I. Dinur, N. Keller, and O. Klein, Fine-grained cryptanalysis: Tight conditional bounds for dense k-SUM and k-XOR, *Journal of the ACM,* **71(3)** (2024), 23, pp. 1-41.

2) O. Dunkelman, N. Keller, E. Ronen, and A. Shamir, The retracing boomerang attack, *Journal of Cryptology,* **37** (2024), 32, pp. 1-42.

3) O. Dunkelman, N. Keller, E. Ronen, and A. Shamir, Quantum time/memory/data tradeoff attacks, *Design, Codes and Cryptography,* **92(1)** (2024), pp. 159-177.

4) O. Dunkelman, M. Eichlseder, D. Kales, N. Keller, G. Leurent, and M. Schofnegger, Practical key-recovery attacks on FLEX-AEAD, *Design, Codes and Cryptography,* **90(4)** (2022), pp. 983-1007.

5) A. Bar-On, I. Dinur, O. Dunkelman, R. Hod, N. Keller, E. Ronen, and A. Shamir, Tight bounds on online checkpointing algorithms, *ACM Transactions on Algorithms,* **16(3)** (2020), pp. 31:1-31:22.

6) A. Bar-On, O. Dunkelman, N. Keller, E. Ronen, and A. Shamir, Improved key recovery attacks on AES with practical data and memory complexities, *Journal of Cryptology,* **33(3)** (2020), pp. 1003-1043.

7) O. Dunkelman, N. Keller, E. Lambooij, and Y. Sasaki, A practical forgery attack on Lilliput-AE, *Journal of Cryptology,* **33(3)** (2020), pp. 910-916.

8) I. Dinur, N. Keller, and O. Klein, An optimal distributed discrete log protocol with applications to homomorphic secret sharing, *Journal of Cryptology,* **33(3)** (2020), pp. 824-873.

9) I. Dinur, O. Dunkelman, N. Keller, and A. Shamir, Efficient dissection of bicomposite problems with cryptanalytic applications, *Journal of Cryptology,* **32(4)** (2019), pp. 1448-1490.

10) A. Bar-On, E. Biham, O. Dunkelman, and N. Keller, Efficient slide attacks, *Journal of Cryptology,* **31(3)** (2018), pp. 641-670.

11) I. Dinur, O. Dunkelman, N. Keller, and A. Shamir, Key-recovery attacks on iterated Even-Mansour encryption schemes, *Journal of Cryptology,* **29(4)** (2016), pp. 697-728.

12) O. Dunkelman, N. Keller, and A. Shamir, Improved single-key attacks on 8-round AES-192 and AES-256, *Journal of Cryptology,* **28(3)** (2015), pp. 397-422.

13) E. Biham, O. Dunkelman, N. Keller, and A. Shamir, New data-efficient attacks on reduced-round variants of IDEA, *Journal of Cryptology,* **28(2)** (2015), pp. 209-239.

14) O. Dunkelman, N. Keller, and A. Shamir, Slidex attacks on the Even-Mansour encryption scheme, *Journal of Cryptology*, **28(1)** (2015), pp. 1-28.

15) I. Dinur, O. Dunkelman, N. Keller, and A. Shamir, Reflections on slide with a twist attacks, *Design, Codes, and Cryptography*, **77(2-3)** (2015), pp. 633-651.

16) O. Dunkelman, N. Keller, and A. Shamir, Almost universal forgery attacks on AES-based MACs, *Design, Codes and Cryptography*, **76(3)** (2015), pp. 431-449.

17) O. Dunkelman and N. Keller, Practical-time attacks on reduced-round Misty1, *Design, Codes and Cryptography*, **76(3)** (2015), pp. 601-627.

18) I. Dinur, O. Dunkelman, N. Keller, and A. Shamir, Dissection: A new paradigm for solving bicomposite search problems, *Communications of the ACM*, **57(10)** (2014), pp. 98-105.

19) 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*, **27(4)** (2014), pp. 824-849.

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

21) 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.

22) 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.

23) 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.

24) 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.

25) 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.

26) 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.

27) 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.

28) 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 Journal 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.

Conference Papers:

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

1) O. Dunkelman, S. Ghosh, N. Keller, G. Leurent, A. Marmor, and V. Mollimard, Partial sums meet FFT: Improved attack on 6-round AES, Eurocrypt (1) 2024, pp. 128-157.

2) O. Dunkelman, N. Keller, and A. Weizmann, Practical-time related-key attack on GOST with secret S-boxes, Crypto (3) 2023, pp. 177-208.

3) I. Dinur, O. Dunkelman, N. Keller, E. Ronen, and A. Shamir, Efficient detection of high-probability statistical properties of cryptosystems via surrogate differentiation, Eurocrypt (4) 2023, pp. 98-127.

4) E. Boyle, I. Dinur, N. Gilboa, Y. Ishai, N. Keller, and O. Klein, Locality-preserving hashing for shifts, with connections to cryptography, ITCS 2022, pp. 27:1-27:24.

5) I. Dinur, N. Keller, and O. Klein, Fine-grained cryptanalysis: Tight conditional bounds for dense k-SUM and k-XOR, FOCS 2021, pp. 80-91.

6) N. Keller and O. Klein, Local concentration inequalities and Tomaszewski's conjecture, STOC 2021, pp. 1656-1669.

7) O. Amon, O. Dunkelman, N. Keller, E. Ronen, and A. Shamir, Three third generation attacks on the Format Preserving Encryption scheme FF3, Eurocrypt (2) 2021, pp. 127-154.

8) N. Keller and A. Rosemarin, Mind the middle layer: The HADES design strategy revisited, Eurocrypt (2) 2021, pp. 35-63.

9) O. Dunkelman, Z. Geyzel, C. Keller, N. Keller, E. Ronen, A. Shamir, and R. Tessler, Error-resilient space partitioning, ICALP 2021, pp. 4:1-4:22.

10) O. Dunkelman, N. Keller, E. Ronen, and A. Shamir, The retracing boomerang attack, Eurocrypt (1) 2020, pp. 280-309.

11) O. Dunkelman, N. Keller, N. Lasry, and A. Shamir, New slide attacks on almost self-similar ciphers, Eurocrypt (1) 2020, pp. 250-279.

12) A. Bar-On, O. Dunkelman, N. Keller, and A. Weizman, DLCT: A new tool for differential-linear cryptanalysis, Eurocrypt (1) 2019, pp. 313-342.

13) A. Bar-On, O. Dunkelman, N. Keller, E. Ronen, and A. Shamir, Improved key recovery attacks on AES with practical data and memory complexities, Crypto (2) 2018, pp. 185-212.

14) I. Dinur, N. Keller, and O. Klein, An optimal Distributed Discrete Log protocol with applications to Homomorphic Secret Sharing, Crypto (3) 2018, pp. 213-242.

15) A. Bar-On, I. Dinur, O. Dunkelman, R. Hod, N. Keller, E. Ronen, and A. Shamir, Tight bounds on online checkpointing algorithms, ICALP 2018, pp. 13.1-13.13.

16) N. Keller and N. Lifshitz, The junta method in extremal hypergraph theory and Chvátal's conjecture, Eurocomb 2017, pp. 711-717. [This paper is in Combinatorics and not in Cryptography.]

17) J. Cho, K.-Y. Choi, I. Dinur, O. Dunkelman, N. Keller, D. Moon, A. Vaidberg, WEM: A new family of white-box block ciphers based on the Even-Mansour construction, CT-RSA 2017, pp. 293-308.

18) J. Cho, K.-Y. Choi, O. Dunkelman, N. Keller, D. Moon, A. Vaidberg, Hybrid WBC: Secure and efficient white-box encryption schemes, CANS 2016, pp. 749-754.

19) A. Bar-On and N. Keller, A 2^70 attack on the full Misty1, Crypto 2016 (1), LNCS 9814, pp. 435-456.

20) I. Dinur, O. Dunkelman, N. Keller, and A. Shamir, Memory-efficient algorithms for finding needles in haystacks, Crypto 2016 (2), LNCS 9815, pp. 185-206.

21) I. Dinur, O. Dunkelman, N. Keller, and A. Shamir, New attacks on Feistel structures with improved memory complexities, Crypto 2015, LNCS 9215, pp. 433-454.

22) A. Bar-On, I. Dinur, O. Dunkelman, N. Keller, V. Lallemand, and B. Tsaban, Cryptanalysis of SP networks with partial non-linear layers, Eurocrypt 2015 (1), LNCS 9056, pp. 315-342.

23) I. Dinur, O. Dunkelman, N. Keller, and A. Shamir, Cryptanalysis of iterated Even-Mansour schemes with two keys, Asiacrypt 2014, LNCS 8873, pp. 439-457.

24) I. Dinur, O. Dunkelman, N. Keller, and A. Shamir, Improved linear sieving techniques, with applications to step-reduced LED-64, FSE 2014, LNCS 8540, pp. 390-410.

25) 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, LNCS 8269, pp. 337-356. (**Solicited for publication in Journal of Cryptology as one of the three best papers**).

26) 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**).

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

28) 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**).

29) 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.

30) 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.

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

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

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

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

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

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

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

38) 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.

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

40) 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.

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

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

43) 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.

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

45) 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.

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

47) 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.

48) 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.

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

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

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

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

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

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

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

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

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

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

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