**Nathen Keller List of 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.*