

# Curriculum Vitae

Palash Sarkar  
Professor  
Applied Statistics Unit  
Indian Statistical Institute

## 1 Academic Degrees

- **Doctor of Philosophy** from the Indian Statistical Institute in 1999.
- **Master of Technology in Computer Science** from the Indian Statistical Institute in 1993.
- **Bachelor of Electronics and Telecommunication Engineering** from Jadavpur University, 1991.

## 2 Academic Experience

- July 2011 onwards: **Professor (HAG)** at the **Indian Statistical Institute**, Kolkata.
- June 2005 – June 2011: **Professor** at the **Indian Statistical Institute**, Kolkata.
- October 2001 – May 2005: **Associate professor** at the **Indian Statistical Institute**, Kolkata.
- September 2000 – September 2001: **Postdoctoral fellow** at the Centre for Applied Cryptographic Research (CACR), **University of Waterloo**.

## 3 Academic Recognition

- Recipient of the **Shanti Swarup Bhatnagar award** for Mathematical Sciences for the year 2011.
- Co-recipient of the **B. M. Birla award** for Mathematics for the year 2005.

## 4 Students Advised

Kaushik Nath (PhD 2021).

Dissertation: Secure and Efficient Computation of the Diffie-Hellman Protocol Using Montgomery Curves over Prime Order Fields.

Madhurima Mukhopadhyay (PhD 2021).

Dissertation: Aspects of Index Calculus Algorithms for Discrete Logarithm and Class Group Computations.

Sebati Ghosh (PhD 2021).

Dissertation: Constructions and Analyses of Efficient Symmetric-Key Primitives for Authentication and Encryption.

Subhabrata Samajder (PhD 2017).

Dissertation: Some Aspects of Statistical Analysis of Linear and Differential Cryptanalysis.

Shashank Singh (PhD 2016).

Dissertation: Studies on Index Calculus Techniques for the Discrete Log Problem.

Sanjay Bhattacharjee (PhD 2015).

Dissertation: Tree-Based Symmetric Key Broadcast Encryption.

Somindu Chaya Ramanna (PhD 2015).

Dissertation: Efficient and Adaptively Secure Constructions of Identity-Based Cryptographic Primitives.

Somitra Kumar Sanadhya (PhD 2009).

Dissertation: A Study of the SHA-2 Cryptographic Hash Family.

Sourav Mukhopadhyay (PhD 2007).

Dissertation: A Study on Time/Memory Trade-Off Cryptanalysis.

Sanjit Chatterjee (PhD 2006).

Dissertation: Construction of (Hierarchical) Identity Based Encryption Protocols Using Bilinear Pairing.

Pradeep Kumar Mishra (PhD 2004).

Dissertation: Studies on Efficient and Secure Implementation of Elliptic and Hyperelliptic Curve Cryptosystems.

Kishan Chand Gupta (PhD 2004).

Dissertation: Cryptographic and Combinatorial Properties of Boolean Functions and S-Boxes.

## Significant Advisory Role.

Subhamoy Maitra (PhD 2001). Advisor: Bimal Kumar Roy.

Dissertation: Boolean Functions with Important Cryptographic Properties.

Ratna Dutta (PhD 2006). Advisor: Rana Barua.

Dissertation: Studies on Pairing-Based and Constant Round Dynamic Group Key Agreement Protocols

Mridul Nandi (PhD 2006). Advisor: Bimal Kumar Roy.

Dissertation: Designs of Iteration on Hash Functions and its Cryptanalysis

## 5 Teaching

### 5.1 Indian Statistical Institute

- **Introduction to Lattices**, Jan-Apr, 2017.
- **Research Methodolgy**, Jan-Apr, 2011.
- **Probability and Stochastic Processes**, Aug-Dec, 2008, 2009, 2010, 2014, 2015, 2016.
- **Topics in Computational Algebra**, Jan–May, 2004, 2005, 2006, 2015, 2016.
- **Information and Coding Theory**, Jan–May, 2006, 2008, 2009.
- **Randomized Algorithms**, research course, Mar–Aug, 2000.
- **Computational Aspects of Cryptography and Coding Theory**, research course, Jan–Apr, 2012.
- **Advanced Topics in Cryptology**, Jan–May, 2004.
- **Cryptology and Data Security**, Aug–Dec, 1999, 2002, 2003.
- **Discrete Mathematics-I (Elements of Algebraic Structures)**, Aug–Dec, 2013, 2012, 2011, 1999.
- **Discrete Mathematics-II (Combinatorics, Graph Theory and Logic)**, Aug–Dec, 1996, 1997, 1998, 2006, 2007.
- **Design and Analysis of Algorithms**, MTech (CS), Jan–May, 1998, 1999, 2002.
- **Selected Topics in Algorithms and Complexity**, MTech (CS), Jan–May, 1999, 2009, 2010.
- **Theory of Automata, Languages, Computability and Complexity**, MTech (CS), Jan–May, 1997, 2000, 2005.
- **Programming in Assembly and Systems Programming**, MTech (CS), Aug-Dec, 1995.

- **Information Storage and Retrieval (C Programming and Database)**, MStat, Aug–Dec, 1996, 1997, 1998.
- **Computational Techniques (C Programming and Numerical Analysis)**, BStat, Jan–May, 1996.
- **Database Management Systems**, Oct–Dec, 2001.
- ORACLE 7.1/FORMS 4.5/REPORTS 2.5, Diploma course, 1995, 1996, 1997.

## 6 Publications

### 6.1 Books

1. Satya R. Chakravarty and Palash Sarkar. *An Introduction to Algorithmic Finance, Algorithmic Trading and Blockchain*. Emerald Publishing Limited, 2020.
2. Satya R. Chakravarty, Manipushpak Mitra and Palash Sarkar. *A Course on Cooperative Game Theory*. Cambridge University Press, 2015.
3. Sanjit Chatterjee and Palash Sarkar. *Identity-Based Encryption*. Springer, 2011. Corrigendum available at <http://www.isical.ac.in/~palash/IBE-book/book-page.html>.

### 6.2 Edited Volumes

1. Palash Sarkar and Tetsu Iwata (editors). **Proceedings of Asiacrypt 2014**, published by **Springer-Verlag** in the **Lecture Notes in Computer Science** series, numbers 8873 and 8874.
2. Kazue Sako and Palash Sarkar (editors). **Proceedings of Asiacrypt 2013**, published by **Springer-Verlag** in the **Lecture Notes in Computer Science** series, numbers 8269 and 8270.
3. Alfred Menezes and Palash Sarkar (editors). **Proceedings of Indocrypt 2002**, published by **Springer-Verlag** in the **Lecture Notes in Computer Science** series, number 2551.

### 6.3 Journal Papers and Papers in Edited Volumes

#### Papers on Cryptology

1. Sebati Ghosh and Palash Sarkar. Breaking Tweakable Enciphering Schemes using Simon’s Algorithm. **Designs, Codes, and Cryptography**, (2021) 89:1907–1926, <https://link.springer.com/article/10.1007/s10623-021-00893-5>.
2. Kaushik Nath and Palash Sarkar. Security and Efficiency Trade-offs for Elliptic Curve Diffie-Hellman at the 128-bit and 224-bit Security Levels. **Journal of Cryptographic Engineering**, <https://link.springer.com/article/10.1007/s13389-021-00261-y>.

3. Kaushik Nath and Palash Sarkar. Efficient 4-way Vectorizations of the Montgomery Ladder. **IEEE Transactions on Computers**, <https://doi.org/10.1109/TC.2021.3060505>.
4. Palash Sarkar and Subhadip Singha. Classical Reduction of GapSVP to LWE: A Concrete Security Analysis. **Advances in Mathematics of Communications**, <https://www.aimsciences.org/article/doi/10.3934/amc.2021004>.
5. Sebati Ghosh and Palash Sarkar. Variants of Wegman-Carter Message Authentication Code Supporting Variable Tag Lengths. **Designs, Codes, and Cryptography**, 89, pages 709–736 (2021), <https://doi.org/10.1007/s10623-020-00840-w>.
6. Kaushik Nath and Palash Sarkar. Reduction Modulo  $2^{448} - 2^{224} - 1$ . **Mathematical Cryptology**, <https://journals.flvc.org/mathcryptology/article/view/123700/127683>.
7. Kaushik Nath and Palash Sarkar. Efficient Arithmetic in (pseudo-)Mersenne Prime Order Fields. **Advances in Mathematics of Communications**, <https://www.aimsciences.org/article/doi/10.3934/amc.2020113>.
8. Debrup Chakraborty, Sebati Ghosh, Cuauhtemoc López and Palash Sarkar. FAST: Disk Encryption and Beyond. **Advances in Mathematics of Communications**, <https://www.aimsciences.org/article/doi/10.3934/amc.2020108>.
9. Madhurima Mukhopadhyay, Palash Sarkar, Shashank Singh and Emmanuel Thomé. New discrete logarithm computation for the medium prime case using the function field sieve. **Advances in Mathematics of Communications**, <https://www.aimsciences.org/article/doi/10.3934/amc.2020119>.
10. Kaushik Nath and Palash Sarkar. Efficient Elliptic Curve Diffie-Hellman Computation at the 256-bit Security Level. **IET Information Security**, volume 14, number 6, 633–640, 2020, DOI: 10.1049/iet-ifs.2019.0620.
11. Sreyosi Bhattacharyya and Palash Sarkar. Improved SIMD Implementation of Poly1305. **IET Information Security**, volume 14, number 5, 521–530, 2020, DOI: 10.1049/iet-ifs.2019.0605.
12. Madhurima Mukhopadhyay and Palash Sarkar. Faster Initial Splitting for Small Characteristic Composite Extension Degree Fields. **Finite Fields and their Applications**, 2020, volume 62, 101629, <http://www.sciencedirect.com/science/article/pii/S1071579719301327>.
13. Palash Sarkar and Subhadip Singha. Verifying Solutions to LWE with Implications for Concrete Security. **Advances in Mathematics of Communications**, May 2021, 15(2): 257–266, <https://www.aimsciences.org/article/doi/10.3934/amc.2020057>.
14. Subhabrata Samajder and Palash Sarkar. Another Look at Success Probability of Linear Cryptanalysis. **Advances in Mathematics of Communications**, November 2019, 13(4): 645–688. DOI: 10.3934/amc.2019040.

15. Sabyasachi Karati and Palash Sarkar. Kummer for Genus One over Prime Order Fields. **Journal of Cryptology**, volume 33, 92–129, 2020, <https://doi.org/10.1007/s00145-019-09320-4>.
16. Palash Sarkar and Shashank Singh. A Unified Polynomial Selection Method for the (Tower) Number Field Sieve Algorithm. **Advances in Mathematics of Communications**, August 2019, 13(3): 435–455. DOI: 10.3934/amc.2019028.
17. Sebati Ghosh and Palash Sarkar. Evaluating Bernstein-Rabin-Winograd Polynomials. **Designs, Codes and Cryptography**, March 2019, Volume 87, Issue 23, 527–546, DOI: 10.1007/s10623-018-0561-7.
18. Sabyasachi Karati and Palash Sarkar. Connecting Legendre with Kummer and Edwards. **Advances in Mathematics of Communications**, February 2019, 13(1): 41–66. DOI: 10.3934/amc.2019003.
19. Subhabrata Samajder and Palash Sarkar. Multiple (Truncated) Differential Cryptanalysis: Explicit Upper Bounds on Data Complexity. **Cryptography and Communications - Discrete Structures, Boolean Functions and Sequences**, November 2018, Volume 10, Issue 6, pages 1137–1163, DOI: <https://doi.org/10.1007/s12095-017-0268-z>.
20. Subhabrata Samajder and Palash Sarkar. Success Probability of Multiple/Multidimensional Linear Cryptanalysis Under General Key Randomisation Hypotheses. **Cryptography and Communications - Discrete Structures, Boolean Functions and Sequences**, September 2018, Volume 10, Issue 5, pages 835–879. DOI: <https://doi.org/10.1007/s12095-017-0257-2>.
21. Debrup Chakraborty, Cuauhtemoc Mancillas-López and Palash Sarkar. Disk Encryption: Do We Need to Preserve Length? **Journal of Cryptographic Engineering**, 8(1): pages 49–69 (2018), DOI: 10.1007/s13389-016-0147-0.
22. Subhabrata Samajder and Palash Sarkar. Rigorous Upper Bounds on Data Complexities of Block Cipher Cryptanalysis. **Journal of Mathematical Cryptology**, 11(3): pages 147–175 (2017), DOI: <https://doi.org/10.1515/jmc-2016-0026>.
23. Debrup Chakraborty, Sebati Ghosh and Palash Sarkar. A Fast Single-Key Two-Level Universal Hash Function. **IACR Transactions on Symmetric Cryptology**, 2017(1): pages 106–128 (2017), DOI: <http://dx.doi.org/10.13154/tosc.v2017.i1.106-128>.
24. Palash Sarkar and Shashank Singh. A simple method for obtaining relations among factor basis elements for special hyperelliptic curves. **Applicable Algebra in Engineering, Communication and Computing**, volume 28, number 2, pages 109–130, 2017.
25. Palash Sarkar and Shashank Singh. A New Method for Decomposition in the Jacobian of Small Genus Hyperelliptic Curves. **Designs, Codes and Cryptography**, 82(3): pages 601–616 (2017), DOI 10.1007/s10623-016-0184-9.

26. Somindu C. Ramanna, Palash Sarkar. Efficient Adaptively Secure IBBE from the SXDH Assumption. **IEEE Transactions on Information Theory**, volume 62, number 10, October 2016, pages 5709–5726.
27. Subhabrata Samajder and Palash Sarkar. Another Look at Normal Approximations in Cryptanalysis. **Journal of Mathematical Cryptology**, 10(2): pages 69–99 (2016), DOI: 10.1515/jmc-2016-0006.
28. Sanjay Bhattacharjee and Palash Sarkar. Reducing Communication Overhead of the Subset Difference Scheme. **IEEE Transactions on Computers**, 65(8): pages 2575–2587 (2016), <http://doi.ieeecomputersociety.org/10.1109/TC.2015.2485231>.
29. Palash Sarkar and Shashank Singh. Fine Tuning the Function Field Sieve Algorithm for the Medium Prime Case. **IEEE Transactions on Information Theory**, volume 62, number 4, April 2016, pages 2233–2253.
30. Debrup Chakraborty and Palash Sarkar. On modes of operations of a block cipher for authentication and authenticated encryption. **Cryptography and Communications - Discrete Structures, Boolean Functions and Sequences**, 8(4): 455-511 (2016), DOI 10.1007/s12095-015-0153-6.
31. Sanjay Bhattacharjee and Palash Sarkar. Tree Based Symmetric Key Broadcast Encryption. **Journal of Discrete Algorithms**, volume 34, 2015, 78–107.
32. Debrup Chakraborty, Cuauhtemoc Mancillas-López and Palash Sarkar. STES: A Stream Cipher Based Low Cost Scheme for Securing Stored Data. **IEEE Transactions on Computers**, volume 64, number 9, September 2015, 2691–2707.
33. Debrup Chakraborty, Vicente Hernandez-Jimenez, Palash Sarkar. Another Look at XCB. **Cryptography and Communications - Discrete Structures, Boolean Functions and Sequences**, volume 7, 2015, 439–468.
34. Palash Sarkar. Modes of Operations for Encryption and Authentication Using Stream Ciphers Supporting an Initialisation Vector. **Cryptography and Communications - Discrete Structures, Boolean Functions and Sequences**, September 2014, Volume 6, Issue 3, pp 189–231.
35. Palash Sarkar. On Some Connections Between Statistics and Cryptology. **Journal of Statistical Planning and Inference**, Volume 148, May 2014, Pages 20–37.
36. Sanjay Bhattacharjee and Palash Sarkar. Concrete Analysis and Trade-Offs for the (Complete Tree) Layered Subset Difference Broadcast Encryption Scheme. **IEEE Transactions on Computers**, Volume 63, Number 7, July 2014, pp 1709–1722.
37. Sanjit Chatterjee and Palash Sarkar. Practical hybrid (hierarchical) identity-based encryption schemes based on the decisional bilinear Diffie-Hellman assumption. **International Journal of Applied Cryptography**, 3(1): 47–83, 2013.

38. Palash Sarkar. A New Multi-Linear Universal Hash Family. **Designs, Codes and Cryptography**, 69(3): 351–367 (2013).
39. Sanjay Bhattacharjee and Palash Sarkar. Complete Tree Subset Difference Broadcast Encryption Scheme and its Analysis. **Designs, Codes and Cryptography**, 66(1-3): 335–362 (2013).
40. Debrup Chakraborty, Cuauhtemoc Mancillas-López, Francisco Rodríguez-Henríquez and Palash Sarkar. Efficient Hardware Implementations of BRW Polynomials and Tweakable Enciphering Schemes. **IEEE Transactions on Computers**, 62(2): 279–294 (2013).
41. Palash Sarkar. Tweakable Enciphering Schemes Using Only the Encryption Function of a Block Cipher. **Information Processing Letters**, volume 111, pages 945–955, 2011.
42. Somindu C. Ramanna and Palash Sarkar. On Quantifying the Resistance of Concrete Hash Functions to Generic Multi-Collision Attacks. **IEEE Transactions on Information Theory**, Volume 57, Issue 7, pp 4798–4816.
43. Palash Sarkar. A Trade-Off Between Collision Probability and Key Size in Universal Hashing Using Polynomials. **Designs, Codes and Cryptography**, Volume 58, Issue 3, 2011, pp 271–278.
44. Palash Sarkar. A Simple and Generic Construction of Authenticated Encryption With Associated Data. **ACM Transactions on Information and Systems Security**, Volume 13 Issue 4, December 2010, Article 33, pp 1–16.
45. Palash Sarkar. Pseudo-Random Functions and Parallelizable Modes of Operations of a Block Cipher<sup>1</sup>. **IEEE Transactions on Information Theory**, Volume 56, Number 8, August 2010, pp 4025–4037.
46. Palash Sarkar. Efficient Tweakable Enciphering Schemes from (Block-Wise) Universal Hash Functions. **IEEE Transactions on Information Theory**, Volume 55, Number 10, October 2009, pp 4749–4760.
47. Palash Sarkar. Domain Extender for Collision Resistant Hash Functions: Improving Upon Merkle-Damgard Iteration. **Discrete Applied Mathematics**, 157 (2009) 1086–1097.
48. Somitra Kumar Sanadhya and Palash Sarkar. A Combinatorial Analysis of Recent Attacks on Step Reduced SHA-2 Family. **Cryptography and Communications - Discrete Structures, Boolean Functions and Sequences**, Volume 1, Number 2/September, 2009, pp 135–282.
49. Kishan Chand Gupta and Palash Sarkar. Computing Partial Walsh Transform from the Algebraic Normal Form of a Boolean Function. **IEEE Transactions on Information Theory**, volume 55, number 3, year 2009, pages 1354–1359.

---

<sup>1</sup>The AE(AD) constructions are incorrect. See <http://eprint.iacr.org/2014/627> for updated schemes and implementation details.



50. Sourav Mukhopadhyay and Palash Sarkar. Hardware Architecture and Cost/time/data Trade-off for Generic Inversion of One-Way Function. **Computación y Sistemas**, Special Issue on Applied Cryptography & Data Security, pp 331–355, Volume 12, No. 3, 2009.
51. Palash Sarkar. A General Mixing Strategy for the ECB-Mix-ECB Mode of Operation. **Information Processing Letters**, 109(2008), 121–123.
52. Debrup Chakraborty and Palash Sarkar. A General Construction of Tweakable Block Ciphers and Different Modes of Operations. **IEEE Transactions on Information Theory**, 54(5): 1991–2006 (2008).
53. Debrup Chakraborty and Palash Sarkar. HCH: A New Tweakable Enciphering Scheme Using the Hash-Counter-Hash Approach. **IEEE Transactions on Information Theory**, 54(4): 1683–1699 (2008).
54. Sanjit Chatterjee and Palash Sarkar. Constant Size Ciphertext HIBE in the Augmented Selective-ID Model and its Extensions. **Journal of Universal Computer Science**, 13(10), 1367–1395, 2007.
55. Palash Sarkar and Subhamoy Maitra. Balancedness and Correlation Immunity of Symmetric Boolean Functions, **Discrete Mathematics**, 307 (2007) 2351–2358.
56. Palash Sarkar. Construction of universal one-way hash functions: Tree hashing revisited. **Discrete Applied Mathematics**, 155(16): 2174-2180 (2007).
57. Palash Sarkar. Masking Based Domain Extenders for UOWHFs: Bounds and Constructions, **IEEE Transactions on Information Theory**, 51(12): 4299–4311.
58. Kishan Chand Gupta and Palash Sarkar, Towards a General Correlation Theorem, **IEEE Transactions on Information Theory**, 51(9): pp. 3297-3302 (2005).
59. Kishan Chand Gupta and Palash Sarkar. Improved Construction of Nonlinear Resilient S-Boxes, **IEEE Transactions on Information Theory**, Volume 51, Number 1, January 2005, pages 339-348.
60. Kishan Chand Gupta and Palash Sarkar. Construction of Perfect Nonlinear and Maximally Nonlinear Multi-Output Boolean Functions Satisfying Higher Order Strict Avalanche Criteria, **IEEE Transactions on Information Theory**, Volume 50, Number 11, November 2004, pages 2886-2893.
61. Palash Sarkar. Domain Extenders for UOWHF: A Finite Binary Tree Algorithm. **Journal of Universal Computer Science**, Volume 11, Number 6, pages 1040–1053.
62. Kishan Chand Gupta and Palash Sarkar. Construction of High Degree Resilient S-boxes With Improved Nonlinearity, **Information Processing Letters**, Volume 95, 2005, pages 413–417.
63. Wonil Lee, Mridul Nandi, Palash Sarkar, Donghoon Chang, Sangjin Lee, Kouichi Sakurai, PGV-Style Block-Cipher-Based Hash Families and Black-Box Analysis. **IEICE Transactions**, 88-A(1): 39-48 (2005).

64. Enes Pasalic, Subhamoy Maitra, Thomas Johansson, and Palash Sarkar, New Constructions of Resilient and Coorelation Immune Boolean Functions Achieving the Upper Bound on Non-linearity, **Journal of Indian Statistical Association**, special issue on cryptology, Volume 42, Number 9, December 2004, pages 287-307.
65. Rana Barua and Palash Sarkar, On the Kernel of First Order Correlation Immune Boolean Functions, **Journal of Indian Statistical Association**, special issue on cryptology, Volume 42, Number 2, December 2004, pages 131-143.
66. Palash Sarkar and Subhamoy Maitra. Construction of Nonlinear Resilient Functions Using “Small” Affine Functions, **IEEE Transactions on Information Theory**, 50(9):2185-2193 (2004).
67. Palash Sarkar and Subhamoy Maitra. Efficient Implementation of Cryptographically Useful Large Boolean Functions, **IEEE Transactions on Computers**, volume 52, number 4, pp 410-417, April 2003.
68. Subhamoy Maitra and Palash Sarkar. Maximum Nonlinearity of Symmetric Boolean Functions on Odd Number of Variables, **IEEE Transactions on Information Theory**, volume 48, number 9, September 2002, pp 2626-2630.
69. Claude Carlet and Palash Sarkar. Spectral Domain Analysis of Correlation Immune and Resilient Boolean Functions, **Finite Fields and their Applications**, Volume 8, Number 1, January 2002, Pages 120-130.
70. Subhamoy Maitra and Palash Sarkar. Characterization of Symmetric Bent Functions – An Elementary Proof, **Journal of Combinatorial Mathematics and Combinatorial Computing**, 43 (2002), 227-230.
71. Subhamoy Maitra and Palash Sarkar. Cryptographically Significant Boolean Functions with Five Valued Walsh Spectra, **Theoretical Computer Science** 276(1-2):133-146 (2002).
72. Palash Sarkar and Subhamoy Maitra. Cross-Correlation Analysis of Cryptographically Useful Boolean Functions and S-Boxes, **Theory of Computing Systems**, 35(1): 39-57 (2002).
73. Subhamoy Maitra and Palash Sarkar. Cryptographic Modifications of Patterson-Weidemann Functions, **IEEE Transactions on Information Theory**, volume 48, number 1, pp. 278-284, 2002.
74. Palash Sarkar. A note on the spectral characterization of correlation immune Boolean functions. **Information Processing Letters**, Volume 74, Numbers 5–6, (2000) pages 191-195.
75. Subhamoy Maitra, Palash Sarkar. Hamming Weights of Correlation Immune Boolean Functions. **Information Processing Letters**, Volume 71, Numbers 3–4, (1999) pages 149–153.
76. Subhamoy Maitra, Bimal K. Roy and Palash Sarkar, Ciphertext only attack on LFSR based encryption scheme, **Bulletin of the Calcutta Statistical Association**, Volume 49, Number 195–196, pages 239-254, 1999.

## Papers on Combinatorial Designs, Boolean Functions and Other Topics

77. Aniruddha Biswas and Palash Sarkar. Separation Results for Boolean Function Classes, **Cryptography and Communications - Discrete Structures, Boolean Functions and Sequences**, 13, pages 451–458 (2021),  
<https://link.springer.com/article/10.1007/s12095-021-00488-w>.
78. Sanjay Burman and Palash Sarkar. An Efficient Algorithm for Software Generation of Linear Binary Recurrences, **Applicable Algebra in Engineering, Communication and Computing**, Volume 15, Issue 3/4, December 2004.
79. Palash Sarkar and Paul J. Schellenberg. Construction of Symmetric Balanced Squares with Blocksize More than One, **Designs, Codes, and Cryptography**, November 2003, Volume 30, Issue 3, pp 235–280.
80. Palash Sarkar, Bimal K. Roy, Pabitra Pal Choudhury and Rana Barua. Polynomial division using left shift register, **Computers and Mathematics with Applications**, Volume 35, Number 6, 1998, pages 27–31.
81. Palash Sarkar and Bimal K. Roy. Construction of Nearly Balanced Uniform Repeated Measurement Designs, **Bulletin of the Calcutta Statistical Association**, Volume 45, Numbers 179–180, pages 235–243, 1995.

## Papers on Voting Games and Inequality Measurement

82. Satya R. Chakravarty and Palash Sarkar. Designing income distributions with specified inequalities. **Economic Theory Bulletin**, to appear.
83. Satya R. Chakravarty and Palash Sarkar. An Inequality Paradox: Relative versus Absolute Indices? **Metron**, 79, pages 241–254 (2021),  
<https://doi.org/10.1007/s40300-021-00206-9>.
84. Satya R. Chakravarty and Palash Sarkar. New Perspectives on the Gini and Bonferroni Indices of Inequality. **Social Choice and Welfare**, 2021,  
<https://doi.org/10.1007/s00355-021-01311-4>.
85. Sanjay Bhattacharjee and Palash Sarkar. Weighted Voting Procedure having a Unique Blocker. **International Journal of Game Theory**, 50, pages 279–295 (2021),  
<https://link.springer.com/article/10.1007/s00182-020-00751-z>.
86. Sanjay Bhattacharjee and Palash Sarkar. Correlation and Inequality in Weighted Majority Voting Games, pp 161–191. In **Festschrift volume in honour of Professor Satya R. Chakravarty**, Indraneel Dasgupta and Manipushpak Mitra (editors), Deprivation, Inequality and Polarization. Economic Studies in Inequality, Social Exclusion and Well-Being, Springer, Singapore, 2019, DOI: [https://doi.org/10.1007/978-981-13-7944-4\\_9](https://doi.org/10.1007/978-981-13-7944-4_9).
87. Rana Barua, Satya R. Chakravarty and Palash Sarkar. Measuring P-Power of Voting. **Journal of Economic Theory and Social Development**, Volume 1, Number 1, Pages 81–91, 2012.

88. Rana Barua, Satya R. Chakravarty and Palash Sarkar. Minimal-Axiom Characterizations of the Coleman and Banzhaf Indices of Voting Power. **Mathematical Social Sciences**, 58 (2009) 367–375.
89. Rana Barua, Satya R. Chakravarty, Sonali Roy and Palash Sarkar. A Characterization and Some Properties of the Banzhaf-Coleman Sensitivity Index, **Games and Economic Behaviour**, Volume 49, Issue 1, October 2004, Pages 31-48.

## Papers on Philosophy

90. Palash Sarkar. Aspects of Inductive Inference in Statistics and Machine Learning. In **A Tribute to the Legend of Professor C. R. Rao**, Indian Statistical Institute Series, Springer, 2021, [https://doi.org/10.1007/978-981-33-6991-7\\_10](https://doi.org/10.1007/978-981-33-6991-7_10).
91. Palash Sarkar. Cārṡākism Redivivus. **Newsletter of the American Philosophical Association on Asian and Asian-American Philosophers and Philosophies**, Fall 2018, pages 26–31.  
<https://cdn.ymaws.com/www.apaonline.org/resource/collection/2EAF6689-4B0D-4CCB-9DC6-FB926D8FF530/AsianV18n1.pdf>.

## Papers on Cellular Automata

92. Palash Sarkar. Computing Shifts in 90/150 Cellular Automata Sequences, **Finite Fields and their Applications**, Volume 9, Issue 2, April 2003, Pages 175-186.
93. Palash Sarkar. A brief history of cellular automata. **ACM Computing Surveys**, Volume 32, Issue 1 (2000), pages 80–107.
94. Palash Sarkar, Rana Barua. Multidimensional Sigma-Automata, Pi-Polynomials and Generalised S-Matrices, **Theoretical Computer Science**, 197(1-2), pages 111–138 (1998).
95. Palash Sarkar and Rana Barua. The set of reversible 90/150 cellular automata is regular, **Discrete Applied Mathematics**, Volume 84, Numbers 1–3, (1998) pages 199-213.
96. Palash Sarkar.  $\sigma^+$ -Automata on Square Grids, **Complex Systems**, Volume 10, pages 121–141, 1998.

## 6.4 Conference Papers

All the papers below have appeared in refereed conference proceedings. The acronym LNCS stands for Lecture Notes in Computer Science, which is a book series published by Springer-Verlag. (Expanded versions of the papers marked with \* have later been published as journal papers and are included in the section on journal papers.)

97. (\*) Sabyasachi Karati and Palash Sarkar. Kummer for Genus One over Prime Order Fields, **Proceedings of Asiacrypt 2017, Part-II**, Lecture Notes in Computer Science, Springer, volume 10625, pages 3–32, 2017. (*This paper was recommended by the program chairs of the conference for invitation to the Journal of Cryptology.*)

98. Palash Sarkar and Shashank Singh, A General Polynomial Selection Method and New Asymptotic Complexities for the Tower Number Field Sieve Algorithm, **Proceedings of Asiacrypt, 2016, Part-I**, Lecture Notes in Computer Science, Springer, volume 10031, pages 36–62, 2016. [http://dx.doi.org/10.1007/978-3-662-53887-6\\_2](http://dx.doi.org/10.1007/978-3-662-53887-6_2).
99. Subhabrata Samajder and Palash Sarkar. A New Test Statistic for Key Recovery Attacks Using Multiple Linear Approximations. **Proceedings of Mycrypt 2016**, Lecture Notes in Computer Science, volume 10311, pages 277–293, 2016.
100. Sanjit Chatterjee, Neal Koblitz, Alfred Menezes, Palash Sarkar. Another Look at Tightness II: Practical Issues in Cryptography. **Proceedings of Mycrypt 2016**, Lecture Notes in Computer Science, volume 10311, pages 21–55, 2016. *Recipient of the best paper award*.
101. Alfred Menezes, Palash Sarkar, Shashank Singh. Challenges with Assessing the Impact of NFS Advances on the Security of Pairing-based Cryptography. **Proceedings of Mycrypt 2016**, Lecture Notes in Computer Science, volume 10311, pages 83–108, 2016.
102. Palash Sarkar and Shashank Singh. New Complexity Trade-Offs for the (Multiple) Number Field Sieve Algorithm in Non-Prime Fields. **Proceedings of Eurocrypt, 2016, Part-I**, Lecture Notes in Computer Science, Springer, volume 9665, pages 429–458, 2016. [http://dx.doi.org/10.1007/978-3-662-49890-3\\_17](http://dx.doi.org/10.1007/978-3-662-49890-3_17).
103. Somindu C. Ramanna and Palash Sarkar. Efficient (Anonymous) Compact HIBE From Standard Assumptions. **Proceedings of the International Conference on Provable Security**, Lecture Notes in Computer Science, volume 8782, pp 243–258, 2014.
104. Subhabrata Samajder and Palash Sarkar. Some Randomness Experiments on TRIVIUM. **Proceedings of the 4th International Conference on Security, Privacy, and Applied Cryptography Engineering**, Lecture Notes in Computer Science, volume 8804, pp 219–236, 2014.
105. Somindu C. Ramanna and Palash Sarkar. Anonymous Constant-Size Ciphertext HIBE From Asymmetric Pairings. **Proceedings of the 14th IMA International Conference on Cryptography and Coding**, Lecture Notes in Computer Science, volume 8308, pages 344–363, 2013.
106. Subhabrata Samajder and Palash Sarkar. Fast Multiplication of the Algebraic Normal Forms of Two Boolean Functions. **Proceedings of the 8th Workshop on Coding and Cryptography**, April 15-19, 2013.
107. Somindu C. Ramanna, Sanjit Chatterjee and Palash Sarkar. Variants of Waters’ Dual System Primitives Using Asymmetric Pairings. **Proceedings of Public Key Cryptography, 2012**, Lecture Notes in Computer Science, volume 7293, pp 298–315.
108. Sanjit Chatterjee, Alfred Menezes and Palash Sarkar. Another Look at Tightness. **Proceedings of Selected Areas in Cryptography, 2011**, Lecture Notes in Computer Science, volume 7118, pages 293–319.

109. Sanjay Bhattacharjee and Palash Sarkar. An Analysis of the Naor-Naor-Lotspeich Subset Difference Algorithm. **Proceedings of the 7th Workshop on Coding and Cryptography**, April 11–15, 2011.
110. Somitra Kumar Sanadhya and Palash Sarkar. A New Hash Family Obtained by Modifying the SHA-2 Family. **Proceedings of ACM Symposium on Information, Computer and Communications Security (ASIACCS '09)**, pages 353–363.
111. (\*) Somitra Kumar Sanadhya and Palash Sarkar. New Collision attacks Against Up To 24-step SHA-2 (extended abstract). **Proceedings of Indocrypt 2008**, Lecture Notes in Computer Science, volume 5365, pages 91–103.
112. (\*) Somitra Kumar Sanadhya and Palash Sarkar. Deterministic Constructions of 21-Step Collisions for the SHA-2 Hash Family. **11th Information Security Conference (ISC 2008)**, Lecture Notes in Computer Science, Springer, volume 5222, pages 244–259.
113. M. Prem Laxman Das and Palash Sarkar. Pairing Computation on Twisted Edwards Form Elliptic Curves. **2nd International Conference on Pairing-Based Cryptography (Pairing 2008)**, Lecture Notes in Computer Science, Springer, volume 5209, pages 192–210.
114. (\*) Somitra Kumar Sanadhya and Palash Sarkar. Non-Linear Reduced Round Attacks Against SHA-2 Hash family. **Australasian Conference on Information Security and Privacy (ACISP 2008)**, Lecture Notes in Computer Science, Springer, volume 5107, pp 254–266.
115. Somitra Kumar Sanadhya and Palash Sarkar. Attacking Reduced Round SHA-256. **Applied Cryptography and Network Security (ACNS 2008)**, Lecture Notes in Computer Science, Springer, volume 5037, pp 130–143.
116. Palash Sarkar. Improving Upon the TET Mode of Operation, **International Conference on Information Security and Cryptology, 2007**, Lecture Notes in Computer Science, Springer, volume 4817, pp 180–192.
117. Somitra Kumar Sanadhya and Palash Sarkar. New Local Collisions for the SHA-2 Hash Family, **International Conference on Information Security and Cryptology, 2007**, Lecture Notes in Computer Science, Springer, volume 4817, pp 192–205.
118. Palash Sarkar and Sanjit Chatterjee. Construction of a Hybrid Hierarchical Identity Based Encryption Protocol Secure Against Adaptive Attacks (Without Random Oracle), **International Conference on Provable Security, 2007**, pp 51–67, Lecture Notes in Computer Science, volume 4784,
119. Pradeep Kumar Mishra, Pinakpani Pal and Palash Sarkar. Towards Minimizing Memory Requirement for Implementation of Hyperelliptic Curve Cryptosystems, **Proceedings of Information Security Practice and Experience Conference (ISPEC 2007)**, LNCS, volume 4464, pp 269–283.
120. Sanjit Chatterjee and Palash Sarkar. HIBE with Short Public Parameters Without Random Oracle, **Proceedings of Asiacrypt, 2006**, LNCS, volume 4284, pp 145–160.

121. Sanjit Chatterjee and Palash Sarkar. New Constructions of Constant Size Ciphertext HIBE Without Random Oracle, **Proceedings of the International Conference on Information Security and Cryptology, 2006**, LNCS, volume 4296, pp 310–327.
122. Sanjit Chatterjee and Palash Sarkar. Multi-Receiver Identity-Based Key Encapsulation with Shortened Ciphertext, **Proceedings of Indocrypt 2006**, LNCS, volume 4329, pp 394–408.
123. Sourav Mukhopadhyay and Palash Sarkar. On the Effectiveness of TMTO and Exhaustive Search Attacks, **Proceedings of the First International Workshop on Security**, LNCS, volume 4266, pp 337–352.
124. (\*) Debrup Chakraborty and Palash Sarkar. HCH: A New Tweakable Enciphering Scheme Using the Hash-Encrypt-Hash Approach, **Proceedings of Indocrypt 2006**, LNCS, volume 4329, pp 287–302.
125. (\*) Debrup Chakraborty and Palash Sarkar. A General Construction of Tweakable Block Ciphers and Different Modes of Operations, **Proceeding of SKLOIS International Conference on Information Security and Cryptology, 2006**, LNCS, volume 4318, pp 88–102.
126. Debrup Chakraborty and Palash Sarkar. A New Mode of Encryption Providing A Tweakable Strong Pseudo-Random Permutation, **Proceedings of Fast Software Encryption, 2006**, LNCS, volume 4047, pp 293–309.
127. Sanjit Chatterjee and Palash Sarkar. Generalization of the Selective-ID Security Model for HIBE Protocols, **Proceedings of Public Key Cryptography, 2006**, LNCS, volume 3958, pp. 241–256.
128. Sanjit Chatterjee and Palash Sarkar. Trading Time for Space: Towards an Efficient IBE Scheme with Short(er) Public Parameters in the Standard Model, **Proceedings of International Conference on Information Security and Cryptology, 2005**, LNCS, volume 3935, pp. 424–440.
129. (\*) Sourav Mukhopadhyay and Palash Sarkar. Hardware Architecture and Trade-Offs for Generic Inversion of One-Way Functions, **Proceedings of the IEEE International Symposium on Circuits and Systems, 2006**, pp 4850–4853.
130. Sourav Mukhopadhyay and Palash Sarkar. Application of LFSRs for Parallel Sequence Generation in Cryptologic Algorithms, **Proceedings of Applied Cryptography and Information Security, 2006**, (as part of the International Conference on Computational Science and its Applications), LNCS, volume 3982, pp. 436–445.
131. Jin Hong and Palash Sarkar. New Applications of Time Memory Data Tradeoffs, **Proceedings of Asiacrypt 2005**, LNCS, volume 3788, pp. 353–372.
132. Alex Biryukov, Sourav Mukhopadhyay and Palash Sarkar. Improved Time-Memory Tradeoffs with Multiple Data, **Proceedings of Selected Areas in Cryptography 2005**, LNCS, 110–127.

133. Sourav Mukhopadhyay and Palash Sarkar, Application of LFSRs in Time/Memory Trade-Off Cryptanalysis, **Proceedings of Workshop on Information Security Applications 2005**, LNCS, 25–37.
134. (\*) Palash Sarkar. Masking Based Domain Extenders for UOWHFs: Bounds and Constructions, **Proceedings of Asiacrypt 2004**, LNCS 3329, pp. 187-200, 2004.
135. Joydip Mitra and Palash Sarkar. Time-Memory Trade-Off Attacks on Multiplications and  $T$ -functions, **Proceedings of Asiacrypt 2004**, LNCS 3329, pp. 468-482, 2004.
136. Sanjit Chatterjee, Palash Sarkar and Rana Barua. Efficient Computation of Tate Pairing in Projective Coordinate Over General Characteristic Fields, **Proceedings of International Conference on Information Security and Cryptology 2004**, LNCS, pp 168–181.
137. Palash Sarkar. HEAD: Hybrid Encryption with Delegated Decryption Capability. **Proceedings of Indocrypt 2004**, LNCS, pp 230-244.
138. Ratna Dutta, Rana Barua and Palash Sarkar. Provably Secure Authenticated Tree Based Group Key Agreement, **Proceedings of International Conference on Information and Communications Security 2004**, LNCS, 92-104.
139. Kishan Chand Gupta and Palash Sarkar. Efficient Representation and Software Implementation of Resilient Maiorana-McFarland S-Boxes, **Proceedings of Workshop on Information Security Applications 2004**, LNCS, 317–331.
140. Palash Sarkar, Pradeep Kumar Mishra and Rana Barua. New Table Look-up Methods for Faster Frobenius Map Based Scalar Multiplication Over  $GF(p^n)$ , **Proceedings of Applied Cryptography and Network Security 2004**, LNCS, 479-493.
141. (\*) Wonil Lee, Mridul Nandi, Palash Sarkar, Donghoon Chang, Sangjin Lee and Kouichi Sakurai. A Generalization of PGV-Hash Functions and Security Analysis in Black-Box Model, **Proceedings of Australasian Conference on Information Security and Privacy 2004**, LNCS, 212-223.
142. Jin Hong, Dong Hoon Lee, Seongtaek Chee and Palash Sarkar. Vulnerability of Nonlinear Filter Generators Based on Linear Finite State Machines, **Proceedings of Fast Software Encryption 2004**, LNCS, 193–209.
143. Pradeep Kumar Mishra and Palash Sarkar. Application of Montgomery’s Trick to Scalar Multiplication for Elliptic and Hyperelliptic Curves Using a Fixed Base Point, **Proceedings of Public Key Cryptography, 2004**, LNCS, 2947, pp 41–54.
144. Palash Sarkar, Pradeep Kumar Mishra and Rana Barua. A Parallel Algorithm for Computing Simultaneous Inversions with Application to Elliptic Curve Scalar Multiplication, **Proceedings of the 46th IEEE International Midwest Symposium on Circuits and Systems**, 2003, pp 782–785.
145. Palash Sarkar. Hiji-bij-bij: A New Stream Cipher with a Self-Synchronizing Mode of Operation, **Proceedings of Indocrypt 2003**, LNCS 2904, pp 36-51.



146. Rana Barua, Ratna Dutta and Palash Sarkar. Extending Joux’s Protocol to Multiparty Key Agreement, **Proceedings of Indocrypt 2003**, LNCS 2904, pp 205-217.
147. (\*) Kishan Chand Gupta and Palash Sarkar. Construction of Perfect Nonlinear and Maximally Nonlinear Multi-Output Boolean Functions Satisfying Higher Order Strict Avalanche Criteria (extended abstract), **Proceedings of Indocrypt 2003**, LNCS 2904, pp 107-120.
148. Pradeep Kumar Mishra and Palash Sarkar. Parallelizing Explicit Formula for Arithmetic in the Jacobian of Hyperelliptic Curves, **Proceedings of Asiacrypt 2003**, LNCS 2894, pp 93-110.
149. Pinakpani Pal and Palash Sarkar. PARSHA-256: A Parallelizable Hash Function and a Multithreaded Implementation, **Proceedings of Fast Software Encryption 2003**, LNCS 2887, February 24-26, 2003.
150. (\*) Kishan Chand Gupta and Palash Sarkar. Improved Construction of Nonlinear Resilient S-Boxes, **Proceedings of Asiacrypt 2002**, LNCS 2501, pp 466-483.
151. Palash Sarkar. The Filter-Combiner Model for Memoryless Synchronous Stream Ciphers, **Proceedings of CRYPTO 2002**, LNCS 2442, pp 533-548.
152. Palash Sarkar and Paul J. Schellenberg. A Parallel Algorithm for Extending Cryptographic Hash Functions, **Proceedings of Indocrypt 2001**, LNCS, pp 40-49.
153. Palash Sarkar and Douglas R. Stinson. Frameproof and IPP Codes, **Proceedings of Indocrypt 2001**, LNCS, 117-126.
154. (\*) Palash Sarkar and Subhamoy Maitra. Efficient Implementation of “Large” Stream Cipher Systems, **Proceedings of Cryptographic Hardware and Embedded Systems 2001**, LNCS, pages 319-332.
155. (\*) Enes Pasalic, Subhamoy Maitra, Thomas Johansson and Palash Sarkar, New Constructions of Correlation Immune and Resilient Boolean Functions Achieving Upper Bounds on Nonlinearity, **Proceedings of Workshop on Coding and Cryptography**, Paris, 2001.
156. Sanjeev Kumar Mishra and Palash Sarkar. Symmetrically Private Information Retrieval, **Proceedings of Indocrypt 2000**, LNCS, Volume 1977, pages 225–236.
157. Palash Sarkar and Subhamoy Maitra. Nonlinearity Bounds and Constructions of Resilient Boolean Functions. **Proceedings of Crypto 2000**, LNCS, pages 515–532.
158. (\*) Palash Sarkar and Subhamoy Maitra. Construction of Nonlinear Boolean Functions with Important Cryptographic Properties. **Proceedings of Eurocrypt 2000**, LNCS, pages 485–506.
159. Subhamoy Maitra and Palash Sarkar, Highly Nonlinear Resilient Functions Optimizing Siegenthaler’s Inequality. **Proceedings of Crypto 1999**, LNCS pages 198–215.

160. Subhamoy Maitra and Palash Sarkar. Enumeration of Correlation Immune Boolean Functions. **Proceedings of Australasian Conference on Information Security and Privacy 1999**, LNCS pages 12–25.
161. Palash Sarkar, Bimal K. Roy, Pabitra Pal Choudhury. VLSI Implementation of Modulo Multiplication Using Carry Free Addition, **Proceedings of the 10th International Conference on VLSI Design 1997**, January 4-7, 1997 Bangalore, India.

## 6.5 Book Chapters and Expository Articles

162. Sanjit Chatterjee and Palash Sarkar. Identity-Based Encryption and Hierarchical Identity-Based Encryption. In **Identity-Based Cryptography**, Cryptology and Information Security Series, Volume 2, editors Marc Joye and Gregory Neven, IOS Press, December 2008, ISBN: 978-1-58603-947-9.
163. Palash Sarkar. Overview of Cryptographic Primitives for Secure Communication. In **Wireless Security and Cryptography: Specifications and Implementations**, CRC-Press, A Taylor and Francis Group, editors, N. Sklavos, X. Zhang, ISBN: 084938771X, 2007.
164. Palash Sarkar. A Sketch of Modern Cryptology: The Art and Science of Secrecy Systems. **Resonance – Journal of Science Education**, volume 5, number 9, September 2000, pp 22–40, Springer India, ISSN 0971-8044 (Print), 0973-712X (Online).

## 6.6 Technical Reports

165. Palash Sarkar and Prasanta S. Bandyopadhyay. Simpson’s Paradox: A Singularity of Statistical and Inductive Inference. <https://arxiv.org/abs/2103.16860>, 2021.
166. Kaushik Nath and Palash Sarkar. Constant Time Montgomery Ladder. **International Association for Cryptologic Research, Cryptology ePrint Archive**, Report 2020/378, <https://eprint.iacr.org/2020/378>.
167. Madhurima Mukhopadhyay, Palash Sarkar. Combining Montgomery Multiplication with Tag Tracing for the Pollard’s Rho Algorithm in Prime Order Fields. **International Association for Cryptologic Research, Cryptology ePrint Archive**, Report 2021/043, <https://eprint.iacr.org/2021/043>.
168. Palash Sarkar. Can Efficient Detection and Isolation Control an Epidemic? <https://arxiv.org/abs/2006.00482>, 2020.
169. Palash Sarkar. A New Blockchain Proposal Supporting Multi-Stage Proof-of-Work. **International Association for Cryptologic Research, Cryptology ePrint Archive**, Report 2019/162, <http://eprint.iacr.org/2019/162>.
170. Subhabrata Samajder and Palash Sarkar. Correlations Between (Nonlinear) Combiners of Input and Output of Random Functions and Permutations. **International Association for Cryptologic Research, Cryptology ePrint Archive**, Report, 2017/1219, <http://eprint.iacr.org/2017/1219>.

171. Palash Sarkar, Shashank Singh, On Irreducible Polynomials of the Form  $b(x^d)$ , <https://arxiv.org/abs/1604.08303>.
172. Subhabrata Samajder and Palash Sarkar. Can Large Deviation Theory be Used for Estimating Data Complexity? **International Association for Cryptologic Research, Cryptology ePrint Archive**, Report 2016/465, <http://eprint.iacr.org/2016/465>.
173. Palash Sarkar. On Approximating Addition by Exclusive OR. **International Association for Cryptologic Research, Cryptology ePrint Archive**, Report 2009/047, <http://eprint.iacr.org/2009/047>.
174. Ratna Dutta and Rana Barua and Palash Sarkar. Pairing-Based Cryptographic Protocols : A Survey. **International Association for Cryptologic Research, Cryptology ePrint Archive**, Report 2004/064, <http://eprint.iacr.org/2004/064>.
175. Palash Sarkar. Pushdown Automaton with the Ability to Flip its Stack. **Electronic Colloquium on Computational Complexity, Technical Report**, TR01-081, 2001, <http://eccc.uni-trier.de/author/02911/>.