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.
  - Awarded the **Indian Statistical Institute Alumni Association Medal** for outstanding performance in MTech (CS), 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**.
- May 1995 – August 2000: **Computer programmer** at the **Indian Statistical Institute**, Kolkata.
- May 1994 - May 1995 : **Computer programmer (Project-Linked)** at the Indian Statistical Institute, Kolkata.
- August 1993 – April 1994: **Associate Information Technology Engineer** at **CMC Ltd.** (a software company), Kolkata.

3 Academic Recognition

Prizes

- Recipient of the **Shanti Swarup Bhatnagar award**[1] for Mathematical Sciences for the year 2011.
- Co-recipient of the **B. M. Birla award**[2] for Mathematics for the year 2005.

Papers

- 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. (*Recommended by the program chairs of the conference for invitation to the Journal of Cryptology.*)
- 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.*

4 Professional Recognition

- Member of the IACR Fellows Selection Committee, 2022 to 2026, chair 2025.
- Honorary Professor, School of Computing, University of Kent, UK, 02/11/2020 to 31/10/2023.
- Program co-chair for Asiacrypt 2014, 2013.
- Program co-chair for Indocrypt 2002.

[1] https://en.wikipedia.org/wiki/Shanti_Swarup_Bhatnagar_Prize_for_Science_and_Technology
[2] https://gpbaasri.org/education-research/b-m-birla-science-prizes-about/

5 Talks

- **Invited speaker** at AgileCrypto 2025, Nha Trang, Vietnam, 2025.
- **Invited speaker** at the Asian Symmetric Key Symposium, Kolkata, India, 2024.
- **Invited speaker** at the International Conference on Cryptology in India, Indocrypt, 2015.
- **Keynote speaker** at International Conference on Electrical Engineering, Computing Science and Automatic Control, CINVESTAV, Mexico City, Mexico, 2015.
- **Invited speaker** at the 18th workshop on Elliptic Curve Cryptography, Chennai, 2014.
- **Invited speaker** at the Workshop on Directions in Authenticated Ciphers, Stockholm, 2012.
- **Invited speaker** at the Asian Symmetric Key Symposium, Singapore, 2011.
- **Invited speaker** at the International Conference on Security Aspects in Information Technology, High-Performance Computing and Networking, Haldia, India, 2011.
- **Invited speaker** at the International Conference on Cryptology in India, Indocrypt, 2008.
- **Invited speaker** at the International Conference on Information Security and Cryptology held at Busan, Korea in 2006.
- **Tutorial speaker** at the International Conference on Cryptology in India, Indocrypt, 2006.
- Delivered many regular talks at leading international conferences across the world.
- Delivered many expository/research talks at various institutes and universities in India.

6 Students Advised

Sreyosi Bhattacharyya (PhD 2025).
Dissertation: Some Studies On Information Set Decoding Algorithms and Universal Hash Functions.

Aniruddha Biswas (PhD 2023).
Dissertation: Studies in Boolean Function Analysis.

Subhadip Singha (PhD 2023).
Dissertation: On the Tightness Gap Analysis of Reductions of some Lattice problems to the Learning with Error problem.

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 Bhattacherjee (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

7 Teaching

7.1 Indian Statistical Institute

- **Number Theory**, Jan-Apr, 2025.
- **Abstract Algebra**, Jan-Apr, 2023, 2024, 2026.
- **Lectures on Algorithmic Issues in Cooperative Game Theory**, Nov, 2017.
- **Lectures on Algorithmic Issues in Finance**, Nov, 2019.
- **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**, 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.
- **Design and Analysis of Algorithms**, BStat, Jul–Nov, 2025.
- **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.

7.2 Other Institutes

- Taught a course on cryptology to students of the **Indian Institute of Technology, New Delhi**, Jan–Apr, 2009.

8 Major Sponsored Projects

8.1 Cryptology

1. **Research and Development of Bilinear Pairing Based Protocols**.
   Funding agency: **Department of Information Technology**.

2. **Block Cipher Design**.
   Funding agency: **Indian Space Research Organisation**.

3. **Implementation of Provably Secure Public Key Protocols**.
   Funding agency: **Indian Statistical Institute**.

4. Team member of a number of other cryptography related projects funded by Government of India.

8.2 Other Projects

1. Team member of a Durgapur Steel Plant funded project on assessing development opportunities for neighbouring population.

2. Team member of a West Bengal Government funded project on techniques for pugmark based estimation of the number of tigers in the Sunderbans.

3. Team member of a West Bengal Government funded project on techniques for estimating elephant population in North Bengal.

4. Team member of a West Bengal Government funded project on audit sampling.

5. Team member of a Government of India funded project on employment prospects of ITI graduates.

9 Major Editorial Work

9.1 Journals

1. **Associate editor** of "Mathematical Cryptology" from Oct 2020 onwards.

2. **Associate editor** of "Journal of Statistical Planning and Inference" for the period 2012–2014.

3. **Associate editor** of "Cryptography and Communications: Discrete Structures and Boolean Functions", from March, 2015 to August 2018.

9.2 Conferences

1. **Program co-chair** (with Professor Tetsu Iwata) for **Asiacrypt 2014**, published by **Springer-Verlag** in the **Lecture Notes in Computer Science** series, numbers 8873 and 8874.

2. **Program co-chair** (with Dr. Kazue Sako) for **Asiacrypt 2013**, published by **Springer-Verlag** in the **Lecture Notes in Computer Science** series, numbers 8269 and 8270.

3. **Program co-chair** (with Professor Alfred Menezes) for the **proceedings of Indocrypt 2002**, published by **Springer-Verlag** in the **Lecture Notes in Computer Science** series, number 2551.

4. **Scientific committee member** for Elliptic Curve Cryptography, 2013, 2012.

5. **Steering committee member** for AgileCrypto 2026.

6. **Program committee member** for
Crypto 2024, 2015, 2012, 2010, 2007; annual North American conference of the *International Association for Cryptologic Research*;
Asiacrypt 2015, 2011, 2008, 2007; annual Asian conference of the *International Association for Cryptologic Research*;
Eurocrypt 2012, 2005; annual European conference of the *International Association for Cryptologic Research*;
Fast Software Encryption (FSE) 2010, 2007, 2005, a workshop of the *International Association for Cryptologic Research*;
Public Key Cryptography (PKC) 2026, a workshop of the *International Association for Cryptologic Research*;
Cryptographers Track – RSA Conference (CT-RSA) 2017, 2016, 2015, 2013, 2005;
Africacrypt 2026, 2025, 2024, 2017, 2016, 2014, 2013, 2011, 2010;
Latincrypt 2010;
Selected Areas in Cryptography, 2024, 2023, 2017, 2016, 2015, 2014;
SKLOIS Conference on Information Security and Cryptology (Inscrypt), 2006;
Applied Cryptography and Network Security (ACNS), 2010, 2009, 2007;
International Conference on Pairing-Based Cryptography (Pairing), 2012, 2007;
International Conference on Information Security and Cryptography (ICISC) 2012, 2011, 2010, 2009, 2008, 2007, 2006, 2005, 2004, 2003;

International Conference on Provable Security (ProvSec) 2012, 2011, 2010, 2009, 2007;
Indocrypt 2015, 2012, 2011, 2009, 2004, 2001, 2000;
Australasian Conference on Information Security and Privacy (ACISP) 2015, 2014, 2012, 2011, 2010, 2009, 2006, 2004;
ACM Symposium on Information, Computer and Communications Security (ASIACCS) 2009;
International Workshop on Security (IWSEC) 2011, 2010, 2009;
Workshop on Coding and Cryptography (WCC), 2019, 2017, 2015, 2011;
Workshop on Boolean Functions and Their Applications (BFA), 2026;
International Conference on Security, Privacy and Applied Cryptographic Engineering (SPACE), 2016;
International Conference on Codes, Cryptology and Information Security (C2SI), 2023, 2019;
International Symposium on Cyber Security, Cryptology and Machine Learning (CSCML), 2024, 2023;
International Conference on Post-Quantum Cryptography (PQCrypto), 2026, 2025, 2024, 2023;
International Conference on Decision and Game Theory for Security (GameSec), 2026, 2025, 2024, 2023;
International Conference on Cryptology, Coding Theory and Cyber Security (I4CS), 2022;
International Conference on Security for Information Technology and Communications (SecITC 2025), 2025; **ACM Conference on Post-Quantum and Quantum-based Security (PQQS)**, 2026.

10 Publications

10.1 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-corrigendum.pdf`.

10.2 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.

10.3 Journal Papers and Papers in Edited Volumes

Papers on Cryptology

1. Claude Carlet and Palash Sarkar. The Nonlinear Filter Model of Stream Cipher Redivivus, **IEEE Transactions on Information Theory**, `https://ieeexplore.ieee.org/document/11569985`.

2. Debrup Chakraborty, Sebati Ghosh, Cuauhtemoc Mancillas López and Palash Sarkar. Implementations of FAST and AEZ on field programmable gate arrays for low level encryption of disks with 4096-byte sectors, **Journal of Cryptographic Engineering**, `https://doi.org/10.1007/s13389-025-00384-6`.

3. Claude Carlet and Palash Sarkar. Use of Simple Arithmetic Operations to Construct Efficiently Implementable Boolean functions Possessing High Nonlinearity and Good Resistance to Algebraic Attacks, **Discrete Applied Mathematics**, `https://www.sciencedirect.com/science/article/pii/S0166218X2500246X`.

4. Madhurima Mukhopadhyay and Palash Sarkar. Pseudo-Random Walk on Ideals: Practical Speed-Up in Relation Collection for Class Group Computation, **Cryptography and Communications - Discrete Structures, Boolean Functions and Sequences**, Volume 17, pages 621–641, (2025).

5. Sreyosi Bhattacharyya, Kaushik Nath and Palash Sarkar. Polynomial hashing over prime order fields. **Advances in Mathematics of Communications**, https://doi.org/10.3934/amc.2024001, 2024.

6. Subhabrata Samajder and Palash Sarkar. Another Look at Key Randomisation Hypotheses. **Designs, Codes, and Cryptography**, https://link.springer.com/article/10.1007/s10623-023-01272-y.

7. Palash Sarkar. A New Blockchain Proposal Supporting Multi-Stage Proof-of-Work. **Journal of Blockchain Research**, volume 1, number 1, 37–50, 2022, https://dx.doi.org/10.4310/JBR.2022.v1.n1.a4.

8. Neal Koblitz, Subhabrata Samajder, Palash Sarkar and Subhadip Singha. Concrete Analysis of Approximate Ideal-SIVP to Decision Ring-LWE Reduction. **Advances in Mathematics of Communications**, https://www.aimsciences.org/article/doi/10.3934/amc.2022082.

9. Palash Sarkar. Computing square roots faster than the Tonelli-Shanks/Bernstein algorithm. **Advances in Mathematics of Communications**, http://www.aimsciences.org/article/doi/10.3934/amc.2022007.

10. Kaushik Nath and Palash Sarkar. Kummer versus Montgomery Face-off over Prime Order Fields. **ACM Transactions on Mathematical Software**, Volume 48, Issue 2, June 2022, 1–28, https://doi.org/10.1145/3503536.

11. 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.

12. 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.

13. 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.

14. 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.

15. 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.

16. Kaushik Nath and Palash Sarkar. Reduction Modulo $2^{448} - 2^{224} - 1$. **Mathematical Cryptology**, https://journals.flvc.org/mathcryptology/article/view/123700/127683.

17. 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.

18. 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.

19. 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.

20. 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.

21. 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.

22. 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.

23. 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.

24. 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.

25. 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.

26. 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.

27. Sebati Ghosh and Palash Sarkar. Evaluating Bernstein-Rabin-Winograd Polynomials. **Designs, Codes and Cryptography**, March 2019, Volume 87, Issue 2–3, 527–546, DOI: 10.1007/s10623-018-0561-7.

28. 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.

29. 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`.

30. 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`.

31. 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.

32. 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`.

33. 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`.

34. 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.

35. 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.

36. 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.

37. 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.

38. Sanjay Bhattacherjee 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`.

39. 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.

40. 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.

41. Sanjay Bhattacherjee and Palash Sarkar. Tree Based Symmetric Key Broadcast Encryption. **Journal of Discrete Algorithms**, volume 34, 2015, 78–107.

42. 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.

43. 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.

44. 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.

45. Palash Sarkar. On Some Connections Between Statistics and Cryptology. **Journal of Statistical Planning and Inference**, Volume 148, May 2014, Pages 20–37.

46. Sanjay Bhattacherjee 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.

47. 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.

48. Palash Sarkar. A New Multi-Linear Universal Hash Family. **Designs, Codes and Cryptography**, 69(3): 351–367 (2013).

49. Sanjay Bhattacherjee and Palash Sarkar. Complete Tree Subset Difference Broadcast Encryption Scheme and its Analysis. **Designs, Codes and Cryptography**, 66(1-3): 335–362 (2013).

50. 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).

51. Palash Sarkar. Tweakable Enciphering Schemes Using Only the Encryption Function of a Block Cipher. **Information Processing Letters**, volume 111, pages 945–955, 2011.

52. 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.

53. 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.

54. 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.

55. Palash Sarkar. Pseudo-Random Functions and Parallelizable Modes of Operations of a Block Cipher[3]. **IEEE Transactions on Information Theory**, Volume 56, Number 8, August 2010, pp 4025–4037.

56. 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.

57. Palash Sarkar. Domain Extender for Collision Resistant Hash Functions: Improving Upon Merkle-Damgard Iteration. **Discrete Applied Mathematics**, 157 (2009) 1086–1097.

58. 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.

59. 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.

60. Sourav Mukhopadhyay and Palash Sarkar. Hardware Architecture and Cost/time/data Tradeoff 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.

61. Palash Sarkar. A General Mixing Strategy for the ECB-Mix-ECB Mode of Operation. **Information Processing Letters**, 109(2008), 121–123.

62. 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).

63. 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).

64. 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.

[3]The AE(AD) constructions are incorrect. See `http://eprint.iacr.org/2014/627` for updated schemes and implementation details.

65. Palash Sarkar and Subhamoy Maitra. Balancedness and Correlation Immunity of Symmetric Boolean Functions, **Discrete Mathematics**, 307 (2007) 2351–2358.

66. Palash Sarkar. Construction of universal one-way hash functions: Tree hashing revisited. **Discrete Applied Mathematics**, 155(16): 2174-2180 (2007).

67. Palash Sarkar. Masking Based Domain Extenders for UOWHFs: Bounds and Constructions, **IEEE Transactions on Information Theory**, 51(12): 4299–4311.

68. Kishan Chand Gupta and Palash Sarkar, Towards a General Correlation Theorem, **IEEE Transactions on Information Theory**, 51(9): pp. 3297-3302 (2005).

69. 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.

70. 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.

71. Palash Sarkar. Domain Extenders for UOWHF: A Finite Binary Tree Algorithm. **Journal of Universal Computer Science**, Volume 11, Number 6, pages 1040–1053.

72. 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.

73. 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).

74. Enes Pasalic, Subhamoy Maitra, Thomas Johansson, and Palash Sarkar, New Constructions of Resilient and Coorelation Immune Boolean Functions Achieving the Upper Bound on Nonlinearity, **Journal of Indian Statistical Association**, special issue on cryptology, Volume 42, Number 9, December 2004, pages 287-307.

75. 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.

76. Palash Sarkar and Subhamoy Maitra. Construction of Nonlinear Resilient Functions Using "Small" Affine Functions, **IEEE Transactions on Information Theory**, 50(9):2185-2193 (2004).

77. 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.

78. 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.

79. 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.

80. Subhamoy Maitra and Palash Sarkar. Characterization of Symmetric Bent Functions – An Elementary Proof, **Journal of Combinatorial Mathematics and Combinatorial Computing**, 43 (2002), 227-230.

81. Subhamoy Maitra and Palash Sarkar. Cryptographically Significant Boolean Functions with Five Valued Walsh Spectra, **Theoretical Computer Science** 276(1-2):133-146 (2002).

82. 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).

83. Subhamoy Maitra and Palash Sarkar. Cryptographic Modifications of Patterson-Weidemann Functions, **IEEE Transactions on Information Theory**, volume 48, number 1, pp. 278-284, 2002.

84. 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.

85. Subhamoy Maitra, Palash Sarkar. Hamming Weights of Correlation Immune Boolean Functions. **Information Processing Letters**, Volume 71, Numbers 3–4, (1999) pages 149–153.

86. 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

87. Aniruddha Biswas and Palash Sarkar. Counting Unate and Monotone Boolean Functions under Restrictions of Balancedness and Non-Degeneracy, **Journal of Integer Sequences**, (2025), Article 25.3.4, `https://cs.uwaterloo.ca/journals/JIS/VOL28/Biswas/biswas6.html`.

88. Aniruddha Biswas and Palash Sarkar. A lower bound on the constant in the Fourier min-entropy/influence conjecture, **Discrete Applied Mathematics**, 364, pages 23–32 (2025), `https://www.sciencedirect.com/science/article/pii/S0166218X24005298`.

89. Aniruddha Biswas and Palash Sarkar. Influence of a Set of Variables on a Boolean Function, **SIAM Journal of Discrete Mathematics**, 37(3), pages 2148–2171 (2023), `https://epubs.siam.org/doi/epdf/10.1137/22M1503531`.

90. Aniruddha Biswas and Palash Sarkar. On The "Majority is Least stable" Conjecture, **Information Processing Letters**, 179, 2023, `https://doi.org/10.1016/j.ipl.2022.106295`.

91. 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.

92. 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.

93. 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.

94. 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.

95. 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 Economics and Voting Games

96. Sanjay Bhattacherjee, Satya R. Chakravarty and Palash Sarkar. A General Model for Multi-Parameter Weighted Voting Games. **International Journal of Game Theory**, https://link.springer.com/article/10.1007/s00182-025-00940-8.

97. Satya R. Chakravarty and Palash Sarkar. Balancing inequality reduction against equality of liabilities in a taxation scheme. **Journal of Mathematical Economics**, 118, (2025), https://www.sciencedirect.com/science/article/abs/pii/S0304406825000217.

98. Sanjay Bhattacherjee and Palash Sarkar. On Using Proportional Representation Methods as Alternatives to Pro-rata Based Order Matching Algorithms in Stock Exchanges. **Computational Economics**, https://doi.org/10.1007/s10614-024-10576-7.

99. Satya R. Chakravarty and Palash Sarkar. Notes on the postulate of the monotonicity in distance in inequality. **Bulletin of Economic Research**, https://doi.org/10.1111/boer.12357.

100. Satya R. Chakravarty and Palash Sarkar. Inequality minimising subsidy and taxation. **Economic Theory Bulletin**, https://link.springer.com/article/10.1007/s40505-022-00218-2.

101. Satya R. Chakravarty and Palash Sarkar. Designing income distributions with specified inequalities. **Economic Theory Bulletin**, https://link.springer.com/article/10.1007/s40505-021-00212-0.

102. 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.

103. 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.

104. Sanjay Bhattacherjee 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.

105. Sanjay Bhattacherjee 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.

106. 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.

107. 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.

108. 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

109. 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.

110. Palash Sarkar. Cārvākism 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

111. Palash Sarkar. Computing Shifts in 90/150 Cellular Automata Sequences, **Finite Fields and their Applications**, Volume 9, Issue 2, April 2003, Pages 175-186.

112. Palash Sarkar. A brief history of cellular automata. **ACM Computing Surveys**, Volume 32, Issue 1 (2000), pages 80–107.

113. Palash Sarkar, Rana Barua. Multidimensional Sigma-Automata, Pi-Polynomials and Generalised S-Matrices, **Theoretical Computer Science**, 197(1-2), pages 111–138 (1998).

114. 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.

115. Palash Sarkar. σ^+-Automata on Square Grids, **Complex Systems**, Volume 10, pages 121–141, 1998.

10.4 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.)

116. Sreyosi Bhattacharyya, Palash Sarkar. Concrete Time/Memory Trade-Offs in Generalised Stern's ISD Algorithm. **Proceedings of Indocrypt 2023**, Lecture Notes in Computer Science, Springer, 307–328.

117. Aniruddha Biswas and Palash Sarkar. Counting unate and balanced monotone Boolean functions. The 8th International Workshop on **Boolean Functions and their Applications (BFA) 2023**.

118. (*) Madhurima Mukhopadhyay and Palash Sarkar. Pseudo-Random Walk on Ideals: Practical Speed-Up in Relation Collection for Class Group Computation. **Proceedings of CSCML 2023**, Lecture Notes in Computer Science, Springer, pages 18–31.

119. Subhabrata Samajder and Palash Sarkar. Correlations Between (Nonlinear) Combiners of Input and Output of Random Functions and Permutations. **Proceedings of CSCML 2023**, Lecture Notes in Computer Science, Springer, pages 181-187.

120. Madhurima Mukhopadhyay and Palash Sarkar. Combining Montgomery Multiplication with Tag Tracing for the Pollard Rho Algorithm in Prime Order Fields. **Proceedings of Security, Privacy, and Applied Cryptography Engineering, 2022**, Lecture Notes in Computer Science, Springer, volume 13783, pages 138–146, 2022.

121. Subhabrata Samajder and Palash Sarkar. Distinguishing Error of Nonlinear Invariant Attacks. **Proceedings of Indocrypt 2022**, Lecture Notes in Computer Science, Springer, volume 13774, pages 319–335, 2022.

122. Sanjay Bhattacherjee and Palash Sarkar. Voting Games to Model Protocol Stability and Security of Proof-of-Work Cryptocurrencies. **Proceedings of the Conference on Decision and Game Theory for Security (GameSec), 2022**, Lecture Notes in Computer Science, Springer, volume 13727, pages 297–318, 2023.

123. (*) 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. (*Recommended by the program chairs of the conference for invitation to the Journal of Cryptology.*)

124. 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`.

125. 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.

126. 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.*

127. 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.

128. 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`.

129. 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.

130. 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.

131. 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.

132. 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.

133. 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.

134. 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.

135. 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.

136. 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.

137. (*) 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.

138. (*) 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.

139. 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.

140. (*) 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.

141. 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.

142. 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.

143. 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.

144. 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,

145. 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.

146. Sanjit Chatterjee and Palash Sarkar. HIBE with Short Public Parameters Without Random Oracle, **Proceedings of Asiacrypt, 2006**, LNCS, volume 4284, pp 145–160.

147. 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.

148. Sanjit Chatterjee and Palash Sarkar. Multi-Receiver Identity-Based Key Encapsulation with Shortened Ciphertext, **Proceedings of Indocrypt 2006**, LNCS, volume 4329, pp 394–408.

149. 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.

150. (*) 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.

151. (*) 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.

152. 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.

153. 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.

154. 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.

155. (*) 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.

156. 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.

157. Jin Hong and Palash Sarkar. New Applications of Time Memory Data Tradeoffs, **Proceedings of Asiacrypt 2005**, LNCS, volume 3788, pp. 353–372.

158. Alex Biryukov, Sourav Mukhopadhyay and Palash Sarkar. Improved Time-Memory Trade-offs with Multiple Data, **Proceedings of Selected Areas in Cryptography 2005**, LNCS, 110–127.

159. 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.

160. (*) Palash Sarkar. Masking Based Domain Extenders for UOWHFs: Bounds and Constructions, **Proceedings of Asiacrypt 2004**, LNCS 3329, pp. 187-200, 2004.

161. 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.

162. 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.

163. Palash Sarkar. HEAD: Hybrid Encryption with Delegated Decryption Capability. **Proceedings of Indocrypt 2004**, LNCS, pp 230-244.

164. 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.

165. 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.

166. 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.

167. (*) 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.

168. 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.

169. 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.

170. 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.

171. 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.

172. Rana Barua, Ratna Dutta and Palash Sarkar. Extending Joux's Protocol to Multiparty Key Agreement, **Proceedings of Indocrypt 2003**, LNCS 2904, pp 205-217.

173. (*) 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.

174. 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.

175. 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.

176. (*) Kishan Chand Gupta and Palash Sarkar. Improved Construction of Nonlinear Resilient S-Boxes, **Proceedings of Asiacrypt 2002**, LNCS 2501, pp 466-483.

177. Palash Sarkar. The Filter-Combiner Model for Memoryless Synchronous Stream Ciphers, **Proceedings of CRYPTO 2002**, LNCS 2442, pp 533-548.

178. Palash Sarkar and Paul J. Schellenberg. A Parallel Algorithm for Extending Cryptographic Hash Functions, **Proceedings of Indocrypt 2001**, LNCS, pp 40-49.

179. Palash Sarkar and Douglas R. Stinson. Frameproof and IPP Codes, **Proceedings of Indocrypt 2001**, LNCS, 117-126.

180. (*) Palash Sarkar and Subhamoy Maitra. Efficient Implementation of "Large" Stream Cipher Systems, **Proceedings of Cryptographic Hardware and Embedded Systems 2001**, LNCS, pages 319-332.

181. (*) 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.

182. Sanjeev Kumar Mishra and Palash Sarkar. Symmetrically Private Information Retrieval, **Proceedings of Indocrypt 2000**, LNCS, Volume 1977, pages 225–236.

183. Palash Sarkar and Subhamoy Maitra. Nonlinearity Bounds and Constructions of Resilient Boolean Functions. **Proceedings of Crypto 2000**, LNCS, pages 515–532.

184. (*) Palash Sarkar and Subhamoy Maitra. Construction of Nonlinear Boolean Functions with Important Cryptographic Properties. **Proceedings of Eurocrypt 2000**, LNCS, pages 485–506.

185. Subhamoy Maitra and Palash Sarkar, Highly Nonlinear Resilient Functions Optimizing Siegenthaler's Inequality. **Proceedings of Crypto 1999**, LNCS pages 198–215.

186. 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.

187. 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.

10.5 Book Chapters and Expository Articles

188. 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.

189. 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.

190. 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).

10.6 Technical Reports

191. Palash Sarkar and Prasanta S. Bandyopadhyay. Simpson's Paradox: A Singularity of Statistical and Inductive Inference. `https://arxiv.org/abs/2103.16860`, 2021.

192. 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`.

193. Palash Sarkar. Can Efficient Detection and Isolation Control an Epidemic? `https://arxiv.org/abs/2006.00482`, 2020.

194. Palash Sarkar, Shashank Singh, On Irreducible Polynomials of the Form $b(x^d)$, `https://arxiv.org/abs/1604.08303`.

195. 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`.

196. 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`.

197. 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`.

198. Palash Sarkar. Pushdown Automaton with the Ability to Flip its Stack. **Electronic Colquium on Computational Complexity, Technical Report**, TR01-081, 2001, `http://eccc.uni-trier.de/author/02911/`.