Curriculum Vitae

Susanta Samanta

Postdoctoral Fellow, Department of Electrical and Computer Engineering
University of Waterloo, Waterloo, Ontario, N2L 3G1, Canada
Email: ssamanta@uwaterloo.ca
Research Profiles: ORCID, Google Scholar, DBLP

Education

Ph.D. in Computer Science, Indian Statistical Institute, Kolkata, India
2017 – 2023
Thesis: Design and Analysis of MDS and Near-MDS Matrices and Their Application to Lightweight Cryptography
Advisor: Prof. Kishan Chand Gupta

M.Sc. in Pure Mathematics, University of Calcutta, Kolkata, India
2014 – 2016

B.Sc. in Mathematics, The University of Burdwan, Burdwan, WB, India
2011 – 2014

Academic Positions

Postdoctoral Fellow
Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, Ontario, N2L 3G1, Canada. *June 2024 – Present*

Visiting Scientist
R. C. Bose Centre for Cryptology and Security, Indian Statistical Institute, 203 B. T. Road, Kolkata 700108, India. *January 2024 – May 2024*

Research Interests

- Zero-Knowledge Proofs Based Post-Quantum Cryptographic Primitives
- Design and Analysis of Diffusion Matrices
- Design and Analysis of Lightweight Cryptographic Primitives
- Coding Theory

Publications

This section lists my research articles published in journals and refereed conferences, as well as preprints under review. Publications are listed in reverse chronological order.

Journal Papers

[1] Kishan Chand Gupta, Sumit Kumar Pandey and **Susanta Samanta**. On the Direct Construction of MDS and Near-MDS Matrices, Advances in Mathematics of Communication, 2026, DOI: http://dx.doi.org/10.3934/amc.2026030.

[2] Yogesh Kumar, **Susanta Samanta**, Prasanna Mishra and Atul Gaur. On the Study of Semi-Involutory and Semi-Orthogonal Matrices, Finite Fields and Their Applications, 110 (2026): 102730, DOI: https://doi.org/10.1016/j.ffa.2025.102730.

[3] Susanta Samanta. On the Counting of Involutory MDS Matrices, Cryptography and Communications, 18 (1): 5–25, 2026, DOI: https://doi.org/10.1007/s12095-024-00756-5.

[4] Yogesh Kumar, Prasanna Mishra, **Susanta Samanta**, Kishan Chand Gupta and Atul Gaur. Construction of all MDS and involutory MDS matrices, Advances in Mathematics of Communications, 19(3): 922–941, 2025, DOI: https://doi.org/10.3934/amc.2024033.

[5] Yogesh Kumar, Prasanna Mishra, **Susanta Samanta**, and Atul Gaur. A systematic construction approach for all 4×4 involutory MDS matrices, Journal of Applied Mathematics and Computing, 70(5): 4677–4697, 2024, DOI: https://doi.org/10.1007/s12190-024-02142-z.

[6] Kishan Chand Gupta, Sumit Kumar Pandey and **Susanta Samanta**. On the Construction of near-MDS Matrices, Cryptography and Communications, 16 (2): 249–283, 2024, DOI: https://doi.org/10.1007/s12095-023-00667-x.

[7] Kishan Chand Gupta, Sumit Kumar Pandey, Indranil Ghosh Ray and **Susanta Samanta**. Cryptographically Significant MDS Matrices over Finite Fields: A Brief Survey and Some Generalized Results, Advances in Mathematics of Communication, 13(4): 779–843, 2019, DOI: https://doi.org/10.3934/amc.2019045.

Conference Papers

[8] Mohammadtaghi Badakhshan, **Susanta Samanta** and Guang Gong. Accelerating Post-quantum Secure zkSNARKs by Optimizing Additive FFT, Selected Areas in Cryptography (SAC) 2025: 339–368, DOI: https://doi.org/10.1007/978-3-032-10536-3_13.

[9] **Susanta Samanta** and Guang Gong. Lumora: A family of permutation based wide-block ciphers for PQC zkSNARK applications, Permutation-based Crypto 2025 Workshop, https://permutationbasedcrypto.org/2025/files/Guang_Gong.pdf.

[10] Prasanna Mishra, Yogesh Kumar, **Susanta Samanta** and Atul Gaur. A New Algorithm for Computing Branch Number of Non-Singular Matrices Over Finite Fields, Security and Cryptography for Networks (SCN) 2024: 187–205, DOI: https://doi.org/10.1007/978-3-031-71073-5_9.

[11] Kishan Chand Gupta, Sumit Kumar Pandey and **Susanta Samanta**. Construction of Recursive MDS Matrices Using DLS Matrices, AFRICACRYPT 2022: 3–27, DOI: https://doi.org/10.1007/978-3-031-17433-9_1.

[12] Kishan Chand Gupta, Sumit Kumar Pandey and **Susanta Samanta**. FUTURE: A Lightweight Block Cipher Using an Optimal Diffusion Matrix, AFRICACRYPT 2022: 28–52, DOI: https://doi.org/10.1007/978-3-031-17433-9_2.

[13] Kishan Chand Gupta, Sumit Kumar Pandey and **Susanta Samanta**. A Few Negative Results on Constructions of MDS Matrices Using Low XOR Matrices, SPACE 2019: 195–213, DOI: https://doi.org/10.1007/978-3-030-35869-3_14.

Preprints

[14] Shakir Ali, Atif Ahmad Khan, Abhishek Kesarwani, **Susanta Samanta**. Quasi-recursive MDS Matrices over Galois Rings, arXiv:2512.17256, 2025, https://arxiv.org/abs/2512.17256.

[15] Yogesh Kumar, **Susanta Samanta** and Atul Gaur. New Insights into Involutory and Orthogonal MDS Matrices, arXiv:2510.05766, 2025, https://arxiv.org/abs/2510.05766.

Teaching Experience

- **ECE 628: Computer Network Security**, University of Waterloo, Delivered two lectures on public-key cryptosystems, **Winter 2026**
- **Coding Theory, M.Tech. CS**, Indian Statistical Institute, Kolkata, Jointly with Prof. Kishan Chand Gupta, **2022**.

Invited Talks

- *Exploring Matrix Structures for Constructing Cryptographically Significant MDS Matrices over Finite Fields*, AMU Algebra with Applications Seminar (AMUAAS), Online, October 1 & 8, 2025.
- *Some Aspects of Boolean Functions and Coding Theory*, Workshop on Combinatorics, Boolean Functions, and Quantum Algorithms in Cryptography, Applied Statistics Unit, Indian Statistical Institute, Kolkata, 11 – 12 January 2024.

Other Talks/Presentations

- **Conference Presentations**
  - *FUTURE: A Lightweight Block Cipher Using an Optimal Diffusion Matrix*, 13th International Conference on Cryptology in Africa (AFRICACRYPT 2022), Fes, Morocco, 18 – 20 July 2022.
  - *Construction of Recursive MDS Matrices Using DLS Matrices*, 13th International Conference on Cryptology in Africa (AFRICACRYPT 2022), Fes, Morocco, 18 – 20 July 2022.
  - *A Few Negative Results on Constructions of MDS Matrices Using Low XOR Matrices*, 9th International Conference on Security, Privacy, and Applied Cryptography Engineering (SPACE 2019), Gandhinagar, India, 3 – 7 December 2019.
- **Other Presentations**
  - *Additive Fast Fourier Transforms and Their Applications to zkSNARK Acceleration*, Ripple Get-Together, University of Waterloo, Waterloo, Canada, 12 September, 2025.

- *An Overview of MILP-Based Approaches to Differential Cryptanalysis*, ComSec Lab Group Crypto Seminar, University of Waterloo, Waterloo, Canada, 10 July 2025.
- *Lumora: A family of permutation based wide-block ciphers for PQC zkSNARK applications*, ComSec Lab Group Crypto Seminar, University of Waterloo, Waterloo, Canada, 12 June 2025.
- *On the Study of Additive Fast Fourier Transforms Over Finite Fields*, ComSec Lab Group Crypto Seminar, University of Waterloo, Waterloo, Canada, 20 March 2025.
- *On the Reduction of Search Space Complexity for Finding MDS Matrices*, Crypto Group Seminar, University of Waterloo, Waterloo, Canada, 31 October 2024.
- *On the Discussion of Pseudo-random Generators*, ComSec Lab Group Crypto Seminar, University of Waterloo, Waterloo, Canada, 2 & 23 October 2024.
- *Additive Fast Fourier Transforms Over Finite Fields*, ComSec Lab Group Crypto Seminar, University of Waterloo, Waterloo, Canada, 22 July 2024.
- *Designing MDS and Near-MDS Matrices and Their Application to Lightweight Cryptography*, ComSec Lab Group Crypto Seminar, University of Waterloo, Waterloo, Canada, 15 July 2024.
- *Some Aspects of Designing MDS and Near-MDS Matrices*, Crypto Group Seminar, University of Waterloo, Waterloo, Canada, 10 July 2024.

Awards and Honors

- Qualified for NBHM M.A./M. Sc. Scholarship for Mathematics, 2015
- INSPIRE Scholarship, 2011–2016

Informal Research Mentorship

- Yogesh Kumar (SAG, DRDO, India). PhD, Department of Mathematics, University of Delhi (2025). Thesis: Algebraic and Combinatorial Study of Cryptographically Significant MDS Matrices

Service and Outreach

- Program Committee: 11th International Workshop on Signal Design and its Applications in Communications (IWSDA 2025).
- Reviewer for journals: *IEEE Transactions on Information Theory, Finite Fields and Their Applications, Designs Codes and Cryptography, Cryptography and Communications, Advances in Mathematics of Communication, etc.*
- Reviewer for conferences: *SAC 2025 (Sub-reviewer), SAC 2024 (Sub-reviewer), IEEE eScience 2024 (Sub-reviewer)*