SANDIP KARMAKAR

20, Vidyasagar Road, Nabagram, Dist.-Hooghly, WB, India – 712246|sandip1kk@gmail.com|+919748042664

EDUCATION

Indian Institute of Technology, Kharagpur, Kharagpur, WB, India

Ph.D. in Computer Science and Engineering, Specialization: Cryptography — **August 2014**

Areas of Research: Cryptology, Side Channel Attacks, Algebraic Attacks

THESIS: SIDE CHANNEL ATTACKS ON STREAM CIPHERS AND COUNTERMEASURES

COURSEWORK: ADVANCED GRAPH THEORY, ARTIFICIAL INTELLIGENCE, EMBEDDED SYSTEMS.

Indian Institute of Technology, Kharagpur, Kharagpur, WB, India

MS (By Research) in Computer Science and Engineering, Specialization: Cryptography — **October 2010**

THESIS: APPLICATION OF CELLULAR AUTOMATA IN DESIGN OF STREAM CIPHERS

COURSEWORK: CRYPTOGRAPHY & NETWORK SECURITY, FOUNDATIONS OF CRYPTOGRAPHY, ADVANCES IN ALGORITHMS, COMPUTATIONAL NUMBER THEORY, ENGLISH FOR TECHNICAL WRITING.

CGPA: 9.76/10

Bengal Engineering and Science University, Howrah, WB, India

BE in Computer Science and Technology — **June 2004**

MARKS: 75.5%

ACHIEVEMENTS

1. RANK – 122 (GENERAL) West Bengal JEE (ENGG.), India.
2. RANK – 72, Percentile 99.77 GATE (CSE), India.
3. Microsoft Research INDIA PhD Fellowship (2012-2015).
4. PhD Guidance: 6 (Completed: 2, Ongoing:4)
5. M.Tech. Guidance: 18 (Completed: 17, Ongoing:1)
6. B.Tech. Guidance: 46 (Completed: 41, Ongoing: 5)

EXPERIENCE

INDUSTRIAL EXPERIENCE

TATA Consultancy Services

Assistant Systems Engineer — **November 2006 – December 2007**

Development of Java/J2ee based web-projects in *financial domain*

TCG Software Services Pvt. Ltd.

Software Engineer — **July 2004 – August 2006**

Development of Java/J2ee based web-projects in banking domain

RESEARCH PROJECT EXPERIENCE

SRIC, IIT Kharagpur, Kharagpur, WB,
Indian Telephone Industry, Bangalore

Research Consultant — **May 2008-December 2010**

Design and Implementation of an Indigenous Encryption System
(FPGA implementation, Language-Verilog)

SRIC, IIT Kharagpur, Kharagpur, WB,
Scientific Analysis Group, DRDO, Delhi

Senior Scientific Officer — **January 2011 – August 2012**

Software Tools for Cryptanalysis of Stream Ciphers
(Language-C, Implemented Cube Attack)

TEACHING EXPERIENCE

TEACHING ASSISTANTSHIPS

IIT Kharagpur, Kharagpur, WB **July 2008-Dec 2013**

1. Computer Architecture Lab (Aug. 2008 - Nov.2008)
2. Switching Circuit Lab (Jan.2009 - May.2009)
3. Cryptography & Network Security [Theory] (Aug.2009 - Nov.2009)
4. Foundations of Cryptography [Theory] (Jan.2010 - May.2010)
5. Programming & Data Structures [Theory] (Aug.2010 - Nov.2010)
6. Operating Systems Lab (Jan.2011 – May 2011)
7. Cryptography & Network Security [Theory] (Aug. 2011 – Nov. 2011)
8. Programming & Data Structure Lab (Jan.2012 – May 2012)
9. Cryptography and Network Security [Theory] (Jul 2012 – Nov 2012)
10. Foundations of Cryptography [Theory] (Jan 2013 – April 2013)
11. Programming & Data Structure [Lab] (Aug. 2013-Nov 2013)

TEACHING

Indian Institute of Information Technology Guwahati
Assistant Professor

July 2014-July 2016

1. Algorithms [Theory] (July 2014-Nov 2014)
2. Database Management Systems [Theory] (January 2015-April 2015)
3. Database Management Systems [Lab] (January 2015-April 2015)
4. Theory of Computation [Theory] (July 2015-Nov 2015)
5. Formal Languages and Automata Theory [Theory] (January 2016-April 2016)
6. Topics in Algorithms [Theory] (January 2016-April 2016)

Indian Institute of Information Technology Kalyani
Assistant Professor

July 2016-Nov 2018

7. Database Management Systems [Theory] (Jul 2016-Nov 2016)
8. Database Management Systems [Lab] (Jul 2016-Nov 2016)
9. Digital Logic [Theory] (July 2016-Nov 2016)
10. Algorithms [Theory] (Jan 2017-April 2017)
11. Compiler Design [Theory] (Jan 2017 – April 2017)
12. Compiler Design [Lab] (Jan 2017 – April 2017)
13. Advanced Algorithms [Theory] (July 2017 – Nov 2017)
14. Operating Systems [Lab] (July 2017 – Nov 2017)
15. Algorithms [Theory] (Jan 2018 – April 2018)
16. Algorithms [Lab] (Jan 2018 – April 2018)
17. Computer Organization and Architecture [Theory] (Jan 2018-April 2018)
18. Computer Organization and Architecture [Lab] (Jan 2018 – April 2018)
19. Advanced Algorithms [Theory] (Jul 2018 – Nov 2018)
20. Computer Organization and Architecture [Lab] (Jul 2018 – Nov 2018)
21. Compiler Design [Lab] (Jul 2018 – Nov 2018)

National Institute of Technology Durgapur
Assistant Professor

Nov 2018- till date

22. Data Structures and Algorithms [Theory] (Jan 2019 – April 2019)
23. Data Structures and Algorithms [Lab] (Jan 2019 – April 2019)
24. Cryptography and Network Security [Theory] (Jan 2019 – April 2019)
25. Microcontroller based Systems [Theory] (July 2019 – Nov 2019)
26. Microcontroller based Systems [Lab] (July 2019 – Nov 2019)
27. Introduction to Computing [Theory] (Jan 2020 – May 2020)
28. Introduction to Computing [Lab] (Jan 2020 – May 2020)
29. Introduction to Computing [Theory] (Jul 2020 – Nov 2020)
30. Introduction to Computing [Lab] (Jul 2020 – Nov 2020)
31. Embedded Systems [Theory] (Jul 2020 – Nov 2020)
32. Embedded Systems [Lab] (Jul 2020 – Nov 2020)
33. Advanced Algorithms [Theory] (Jan 2021 – May 2021)
34. Signals and Systems [Theory] (Jan 2021 – May 2021)
35. Signals and Systems [Lab] (Jan 2021 – April 2021)
36. Embedded Systems [Theory] (Aug 2021- Nov 2021)
37. Embedded Systems [Lab] (Aug 2021-Nov 2021)
38. Signals and Systems [Theory] (Jan 2022-Apr 2022)
39. Signals and Systems [Lab] (Jan 2022-Apr 2022)

40. Advanced Algorithms [Theory] (Jan 2022-Apr 2022)
41. Embedded Systems [Theory] (Jul 2022 – Nov 2022)
42. Embedded Systems [Lab] (Jul 2022 – Nov 2022)
43. Advanced Algorithms [Theory] (Jan 2023 – Apr 2023)
44. Introduction to C Programming [Lab] (Jul 2023 – Nov 2023)
45. Discrete Mathematics [Theory] (Jul 2023 – Nov 2023)
46. Advanced Algorithms [Theory] (Jan 2024 – Apr 2024)
47. Data Structures and Algorithms [Lab] (Jan 2024 – Apr 2024))
48. Compiler Design [Theory] (Jul 2024 – Nov 2024)
49. Introduction to C Programming [Lab] (Jul 2024 – Nov 2024)
50. Theory of Computation [Theory] (Jan 2025 – Apr 2025)
51. Advanced Algorithms [Theory] (Jan 2025 – Apr 2025)
52. Compiler Design [Lab] (Jan 2025 – Apr 2025)
53. Compiler Design [Theory] (Jul 2025 – Nov 2025)
54. Compiler Design [Lab] (Jul 2025 – Nov 2025)
55. Computational Number Theory [Theory] (Jan 2026 – Apr 2026)
56. Data Structures and Algorithms [Lab] (Jan 2026 – Apr 2026)
57. Computability and Complexity Theory [Theory] (Jul 2026 – Nov 2026)
58. Computer Programming [Lab] (Jul 2026 – Nov 2026)

PUBLICATIONS AND PAPERS

JOURNALS

1. Sandip Karmakar, Dipanwita Roy Chowdhury: Design and Analysis of Some Cryptographically Robust Non-uniform Nonlinear Cellular Automata. J. Cellular Automata 13(1-2): 145-158 (2018)

2. Sandip Karmakar: An Experiment with Some Rule 30 and Rule 150 Hybrid Non-linear 461Cellular Automata for Cryptography. J. Cellular Automata 13(5-6): 461-477 (2018)

3. Sandip Karmakar, Dipanwita Roy Chowdhury: Scan-based side channel attack on stream ciphers and its prevention. J. Cryptographic Engineering 8(4): 327-340 (2018)

4. Sandip Karmakar, Dipanwita Roy Chowdhury: Leakage Squeezing Using Cellular Automata and Its Application to Scan Attack. J. Cellular Automata 9(5-6): 417-436 (2014)

5. Sandip Karmakar, Debdeep Mukhopadhyay, Dipanwita Roy Chowdhury: CAvium - Strengthening Trivium Stream Cipher Using Cellular Automata. J. Cellular Automata 7(2): 179-197 (2012)

6. An algebraic cryptanalysis tool for cube attack on symmetric ciphers: S Karmakar, P Mishra, N Gaba, DR Chowdhury. Journal of Information and Optimization Sciences 39 (6), 1231-1243

7. S. Basu, D. Bera and S. Karmakar, "Detection and Intelligent Control of Cloud Data Location using Hyperledger Framework," in IEEE Transactions on Consumer Electronics, 2022, doi: 10.1109/TCE.2022.3201932.

8. Basu, S., Karmakar, S. and Bera, D., 2022. Securing Cloud Virtual Machine Image Using Ethereum Blockchain. International Journal of Information Security and Privacy (IJISP), 16(1), pp.1-22.

9. Lama, R., Karmakar, S. Secure waste collection approach for smart cities. Int. j. inf. tecnol. 16, 2439–2454 (2024). https://doi.org/10.1007/s41870-024-01751-y.

10. Lama, R., Karmakar, S. IFTTT-based secure smart farming monitoring system: data integrity and agricultural optimization. Int. j. inf. tecnol. 16, 3649–3662 (2024). https://doi.org/10.1007/s41870-024-01894-y

11. Lama, R., & Karmakar, S. (2024). Secure three-tier authentication approach for agricultural internet of things. Cyber-Physical Systems, 1–24. https://doi.org/10.1080/23335777.2024.2372583

12. Lama R, Karmakar S. SiSMA-SWMS: Signature-based Secure Monitoring Approach for Smart Waste Monitoring Systems. Security and Privacy. 2024; 7(5):e405. doi: 10.1002/spy2.405

13. Radhika Lama, Sandip Karmakar: STccAMTS: secure traffic congestion control approach for marine transportation system. Int. J. Ad Hoc Ubiquitous Comput. 49(2): 92-104 (2025)

14. Radhika Lama and Sandip Karmakar, "CoSMT-LC: Secure Collaborative Marine Traffic Management using Lightweight Cryptography", in *IEEE Internet of Things Journal*, vol. 13, no. 11, pp. 22708-22725, 1 June, 2026, doi: 10.1109/JIOT.2026.3662363.

CONFERENCES

15. R. Dutta, S. Karmakar, Understanding the impact of ransomware attack: A comprehensive study on evolution, detection and prevention techniques, challenges. Selected as "Poster Presentation" in Workshop on Information Security and Privacy (WISP), ICIS (2023), Hyderabad.

16. R. Dutta, S. Karmakar, Ransomware Detection in Healthcare Organizations using Supervised Learning Models: Random Forest Technique. in 4th International Conference on "Emerging Trends and Technologies on Intelligent Systems" (ETTIS – 2024), CDAC,Noida. Lecture Notes in Networks and Systems (Springer).

17. R. Dutta, S. Karmakar, "Ransomware Detection in Healthcare Organizations using Supervised Learning Models: Naïve Bayes Classifier". in 15th International IEEE Conference on Computing Communication and Networking Technologies, 15th ICCCNT2024, IIT MANDI. (Published).

18. S. Sankar, R. Dutta, S. Karmakar, "Cyber Threat Prediction and Assessment with Machine Learning Approaches". in INDICON 2024, IIT Kharagpur.

19. R. Lama, S. K. Singh and S. Karmakar, "Cloud-Based Secure Vehicular Navigation System: Ensuring Privacy and Security in Intelligent Transportation," 2023 International Conference on Electrical, Computer and Energy Technologies (ICECET), Cape Town, South Africa, 2023, pp. 1-6, doi: 10.1109/ICECET58911.2023.10389296.

20. Ms. Srijita Basu, Ms. Shubhasri Roy, Dr. Debasish Bera and Dr. Sandip Karmakar. Hyperledger based Verifiable and Secure Cloud Data Deletion: IEEE INFOCOM WKSHPS: ICCN 2023: IEEE International Workshop on Intelligent Cloud Computing and Networking.

21. R. Lama and S. Karmakar, "Lightweight Authentication approach for Marine Internet of Things," 2022 International Conference on Electrical, Computer and Energy Technologies (ICECET), Prague, Czech Republic, 2022, pp. 1-6, doi: 10.1109/ICECET55527.2022.9872803.

22. K. Jamuda, R. Lama and S. Karmakar, "A Secured Scheme for Optimal Navigation of a Berthing Ship," 2022 International Conference on Electrical, Computer and Energy Technologies (ICECET), Prague, Czech Republic, 2022, pp. 1-6, doi: 10.1109/ICECET55527.2022.9872741.

23. R. Lama and S. Karmakar, "The Cost-Effective Secure and Privacy-preserving Navigation System," 2021 12th International Conference on Computing Communication and Networking Technologies (ICCCNT), Kharagpur, India, 2021, pp. 1-7, doi:10.1109/ICCCNT51525.2021.9580128.

24. R. Lama and S. Karmakar, "The Secure and Privacy-Preservation for Navigation Service Scheme in Marine-based Internet of Things," 2021 International Conference on Electrical, Computer and Energy Technologies (ICECET), Cape Town, South Africa, 2021, pp. 1-6, doi:10.1109/ICECET52533.2021.9698777.

25. R. Lama and S. Karmakar, "3-way Authentication Approach for Agricultural IOT using IFTTT application," 2021 12th International Conference on Computing Communication and Networking Technologies (ICCCNT), Kharagpur, India, 2021, pp. 1-7, doi:10.1109/ICCCNT51525.2021.9579958.

26. R. Lama and S. Karmakar. Secure and Privacy-Preserving UAV-based Rescue Operations for Vehicles in Rugged Terrain (Submitted)

27. Srijita Basu, Sandip Karmakar and Debashis Bera. Blockchain Based Secure Virtual Image Monitor. ICISSP 2021, 432-439.

28. Sandip Karmakar and Dipanwita Roy Chowdhury. Differential Fault Analysis of MICKEY-128 2.0. IEEE FDTC 2013. 52-59, Santa Barbara, CA, USA, 20th August, 2013.

29. Sandip Karmakar and Dipanwita Roy Chowdhury. NOCAS: A Nonlinear Cellular Automata Based Stream Cipher. Automata 2011, 17th International Workshop on Cellular Automata and Discrete Complex Systems,135-146. November 21-23, 2011, Santiago, Chile.

30. Sandip Karmakar and Dipanwita Roy Chowdhury. Fault Analysis of Grain-128 by Targeting NFSR. Africacrypt 2011, 298-315, July 5-7, 2011, Dakar, Senegal.

31. Sandip Karmakar, Debdeep Mukhopadhyay and Dipanwita Roy Chowdhury. Cube Attack on a Simplified version of Trivium. National Workshop of Cryptology 2010, Coimbatore, India. (Presented)

32. Sandip Karmakar, Debdeep Mukhopadhyay and Dipanwita Roy Chowdhury. d-monomial Tests on Nonlinear Cellular Automata for Cryptographic Design. ACRI 2010,261-270. Ascoli Piceno, Italy, September 2010.

33. Sandip Karmakar, Debdeep Mukhopadhyay and Dipanwita Roy Chowdhury. CAvium - Strengthening Trivium using Cellular Automata. Automata 2010, Nancy, France, June 2010.

34. Sandip Karmakar, Debdeep Mukhopadhyay and Dipanwita Roy Chowdhury. A New Cellular Automata Ruleset for Cryptographic Pseudorandom Sequence Generation. National Workshop of Cryptology 2009, SVNIT, Surat, India. (Presented)

35. Sandip Karmakar and Dipanwita Roy Chowdhury. Leakage Squeezing using Cellular Automata. Gieben, Germany, Automata 2013,98-109. Giessen, Germany, September 2013.(Presented)

36. Sandip Karmakar and Dipanwita Roy Chowdhury. Countermeasures of Side Channel Attacks on Symmetric Key Ciphers using Cellular Automata. ACRI 2012.623-632, Santorini, Greece.

37. Mukesh Agrawal, Sandip Karmakar, Dhiman Saha and Debdeep Mukhopadhayay. Scan Based Side Channel Attacks on Stream Ciphers and their Counter-measures. Progress in Cryptology - INDOCRYPT 2008, Volume 5365/2008, pages 226-238, December 2008, Kharagpur, India.

38. Dhiman Saha, Sandip Karmakar, Debdeep Mukhopadhyay and Dipanwita Roy Chowdhury. An FPGA implementation of the Trivium Stream Cipher. National Workshop of Cryptology 2008, Hyderabad, India.

Last Updated: 29th October, 2026