Souradyuti Paul

Professor, Department of Computer Science and Engineering,
Indian Institute of Technology Bhilai

Office 405B, ED1 Building
Department of Computer Science & Engineering
IIT Bhilai, Chhattisgarh 491002, India

+91 82380 50231
souradyuti@iitbhilai.com
souradyutip.github.io

RESEARCH INTERESTS

Cryptographic modes and multiparty protocols; blockchain and cryptocurrency; anonymity and privacy; network security.

PROFESSIONAL EXPERIENCE

Professor, Computer Science and Engineering, IIT Bhilai — Mar 2026 – present

Associate Professor, Computer Science and Engineering, IIT Bhilai — Oct 2017 – Mar 2026

Assistant Professor, Computer Science and Engineering, IIT Gandhinagar — Jul 2014 – Oct 2017

Postdoctoral Researcher, Dept. of Combinatorics & Optimization and David R. Cheriton School of Computer Science, University of Waterloo, Canada — 2012 – 2014
Mentors: Prof. Alfred Menezes and Prof. Douglas Stinson

Guest Researcher, Computer Security Division, National Institute of Standards and Technology (NIST), USA — 2008 – 2012
Project: evaluation of the US Government hash standard SHA-3

Postdoctoral Researcher, KU Leuven, Belgium — 2006 – 2008
Mentor: Prof. Bart Preneel

Assistant Systems Engineer, Tata Consultancy Services (TCS), India — 1998 – 1999

EDUCATION

Ph.D. in Cryptology and Data Security, KU Leuven, Belgium — 2006
Thesis: *Cryptanalysis of Stream Ciphers Based on Arrays and Modular Addition*
Advisor: Prof. Bart Preneel

M.Tech. in Computer Science, Indian Statistical Institute — 2001
Thesis: *Study of Non-linearity of Certain Boolean Functions*
Advisor: Prof. Subhamoy Maitra

B.E. in Mechanical Engineering, Jadavpur University, India — 1998
Minor: Advanced Algebra

AWARDS AND HONOURS

Nominated to the steering committee of the nationwide ACM India Cybersecurity Initiative — 2021

Nominated to lead multiple Indian initiatives, organised by the Bureau of Indian Standards, for standardising blockchain-based applications under various ISO projects — 2019

Invited as a judge at the Smart India Hackathon; certificate from the Ministry of Education for exceptional contribution — 2019

Excellence in Research Fellowship, IIT Gandhinagar — 2014

Member of the evaluation committee for the US Government cryptographic hash function standard SHA-3 — 2008 – 2012

Ranked 111 out of 100,000+ (99.9th percentile), West Bengal Joint Entrance Examination — 1994

Indian National Mathematical Olympiad (INMO) Award, All-India rank 26, presented by the National Board for Higher Mathematics (NBHM), India — 1992

PUBLICATIONS IN FULLY PEER-REVIEWED JOURNALS, BOOK SERIES AND CONFERENCES

1. **Souradyuti Paul**, Devansh Shrivastava. *Energy Trading Using Blockchain at IIT Bhilai Campus.* ISEA Annual Magazine, 2026 (accepted, to appear).
2. Kolichala Rajashekar, **Souradyuti Paul**, Sushanta Karmakar, Subhajit Sidhanta. *Reinforcement Learning for Real-Time Federated Learning for Resource-Constrained Edge Cluster.* Journal of Network and Systems Management 32:94, 2024. doi:10.1007/s10922-024-09857-1
3. Kolichala Rajashekar, Subhajit Sidhanta, **Souradyuti Paul**. *Towards a Mobility-cum-Battery Aware Dynamic UAV Deployment for Uninterrupted Connectivity.* NOMS 2024, pp. 1–5. doi:10.1007/978-3-031-63992-0_5
4. Kolichala Rajashekar, **Souradyuti Paul**, Sushanta Karmakar, Subhajit Sidhanta. *Minimizing Data Retrieval Delay in Edge Computing.* MobiQuitous (2) 2023, pp. 63–85. doi:10.1007/978-3-031-63992-0_5
5. Kolichala Rajashekar, Sushanta Karmakar, **Souradyuti Paul**, Subhajit Sidhanta. *Topology-Aware Cluster Configuration for Real-time Multi-access Edge Computing.* 24th International Conference on Distributed Computing and Networking (ICDCN) 2023, Kharagpur, India, January 4–7, 2023, pp. 286–287. ACM. doi:10.1145/3571306.3571417
6. Arti Dhiman, **Souradyuti Paul**. *Blockchain-based E-voting: A Status Update.* India Internet Governance Forum (IIGF) 2023. press release
7. Kolichala Rajashekar, **Souradyuti Paul**, Sushanta Karmakar, Subhajit Sidhanta. *Topology Aware Cluster Configuration for Minimizing Communication Delay in Edge Computing.* 42nd IEEE International Conference on Distributed Computing Systems (ICDCS) 2022, Bologna, Italy, July 10–13, 2022, pp. 1310–1311. IEEE. doi:10.1109/ICDCS54860.2022.00144
8. **Souradyuti Paul**, Ananya Shrivastava. *Efficient Fair Multiparty Protocols using Blockchain and Trusted Hardware.* In Peter Schwabe and Nicolas Thériault, eds., 6th International Conference on Cryptology and Information Security in Latin America (Latincrypt), LNCS 11774, pp. 301–320. Springer, Cham, 2019. doi:10.1007/978-3-030-30530-7_15
9. Suyash Kandele, **Souradyuti Paul**. *Key Assignment Scheme with Authenticated Encryption.* IACR Transactions on Symmetric Cryptology 2018(4):150–196, 2018. doi:10.13154/tosc.v2018.i4.150-196
10. **Souradyuti Paul**, Ananya Shrivastava. *Robust Multiparty Computation with Faster Verification Time.* In Willy Susilo and Guomin Yang, eds., 23rd Australasian Conference on Information Security and Privacy (ACISP) 2018, LNCS 10946, pp. 114–131. Springer, Cham, 2018. doi:10.1007/978-3-319-93638-3_8
11. Suyash Kandele, **Souradyuti Paul**. *Message-Locked Encryption with File Update.* In Bart Preneel and Frederik Vercauteren, eds., 16th International Conference on Applied Cryptography and Network Security (ACNS) 2018, LNCS 10892, pp. 678–695. Springer, Cham, 2018. doi:10.1007/978-3-319-93387-0_35
12. Indra Deep Mastan, **Souradyuti Paul**. *A New Approach to Deanonymization of Unreachable Bitcoin Nodes.* In Srdjan Čapkun and Sherman S. M. Chow, eds., Cryptology and Network Security (CANS) 2017, LNCS 11261, pp. 277–298. Springer, Cham, 2017. doi:10.1007/978-3-030-02641-7_13
13. Sudhakar Kumawat, **Souradyuti Paul**. *A New Constant-size Accountable Ring Signature Without Random Oracles.* In Xiaofeng Chen and Moti Yung, eds., Inscrypt 2017, LNCS 10726, pp. 157–179. Springer, Cham, 2017. doi:10.1007/978-3-319-75160-3_11
14. Dustin Moody, **Souradyuti Paul**, Daniel Smith-Tone. *Indifferentiability Security of the Fast Wide Pipe Hash: Breaking the Birthday Barrier.* Journal of Mathematical Cryptology 10(2):101–133. De Gruyter, 2016. doi:10.1515/jmc-2014-0044
15. Dustin Moody, **Souradyuti Paul**, Daniel Smith-Tone. *Improved Indifferentiability Security Bound for the JH Mode.* Designs, Codes and Cryptography 79(2):237–259, 2016. doi:10.1007/s10623-015-0047-9
16. **Souradyuti Paul**, Ekawat Homsirikamol, Kris Gaj. *A Novel Permutation-based Hash Mode of Operation FP and the Hash Function SAMOSA.* In Steven Galbraith and Mridul Nandi, eds., Indocrypt 2012, LNCS 7668, pp. 514–532. Springer, 2012. doi:10.1007/978-3-642-34931-7_29
17. Dustin Moody, **Souradyuti Paul**, Daniel Smith-Tone. *Improved Indifferentiability Security Bound for the JH Mode* (extended abstract). 3rd SHA-3 Candidate Conference, 2012. NIST event page
18. Shu-jen Chang, Ray Perlner, William Burr, Meltem Sönmez Turan, John M. Kelsey, **Souradyuti Paul**, Lawrence E. Bassham. *Third-Round Report of the SHA-3 Cryptographic Hash Algorithm Competition.* NIST IR 7896, Department of Commerce, Government of the USA, 2012. doi:10.6028/NIST.IR.7896
19. Meltem Sönmez Turan, Ray Perlner, Lawrence E. Bassham, William Burr, Donghoon Chang, Shu-jen Chang, Morris J. Dworkin, John M. Kelsey, **Souradyuti Paul**, Rene Peralta. *Status Report on the Second Round of the SHA-3 Cryptographic Hash Algorithm Competition.* NIST IR 7764, Department of Commerce, Government of the USA, 2011. doi:10.6028/NIST.IR.7764
20. Mridul Nandi, **Souradyuti Paul**. *Speeding up the Wide-pipe: Secure and Fast Hashing.* In Guang Gong and Kishan Chand Gupta, eds., Indocrypt 2010, LNCS 6498, pp. 144–162. Springer, 2010. doi:10.1007/978-3-642-17401-8_12
21. Andrew Regenscheid, Ray Perlner, Shu-jen Chang, John Kelsey, Mridul Nandi, **Souradyuti Paul**. *Status Report on the First Round of the SHA-3 Cryptographic Hash Algorithm Competition.* NIST IR 7620, Department of Commerce,

Government of the USA, 2009. doi:10.6028/NIST.IR.7620

22. Gautham Sekar, **Souradyuti Paul**, Bart Preneel. *New Attacks on the Stream Cipher TPy6 and Design of New Ciphers the TPy6-A and the TPy6-B.* In Stefan Lucks, Ahmad-Reza Sadeghi and Christopher Wolf, eds., WEWoRC 2007, LNCS 4945, pp. 127–141. Springer, 2007. doi:10.1007/978-3-540-88353-1_11
23. Gautham Sekar, **Souradyuti Paul**, Bart Preneel. *New Weaknesses in the Keystream Generation Algorithms of the Stream Ciphers TPy and Py.* In Juan A. Garay, Arjen K. Lenstra, Masahiro Mambo and René Peralta, eds., ISC 2007, LNCS 4779, pp. 249–262. Springer, 2007. doi:10.1007/978-3-540-75496-1_17
24. Gautham Sekar, **Souradyuti Paul**, Bart Preneel. *Related-Key Attacks on the Py-Family of Ciphers and an Approach to Repair the Weaknesses.* In K. Srinathan, C. Pandu Rangan and Moti Yung, eds., Indocrypt 2007, LNCS 4859, pp. 58–72. Springer, 2007. doi:10.1007/978-3-540-77026-8_6
25. **Souradyuti Paul**, Bart Preneel. *On the (In)security of Stream Ciphers Based on Arrays and Modular Addition.* In Xuejia Lai and Kefei Chen, eds., Asiacrypt 2006, LNCS 4284, pp. 69–83. Springer, 2006. doi:10.1007/11935230_5
26. **Souradyuti Paul**, Bart Preneel, Gautham Sekar. *Distinguishing Attacks on the Stream Cipher Py.* In Matthew J. B. Robshaw, ed., FSE 2006, LNCS 4047, pp. 405–421. Springer, 2006. doi:10.1007/11799313_26
27. **Souradyuti Paul**. *Cryptology: A Mathematician's Quest for Making and Breaking the Code.* In Sanatan Paul, Saroj Kumar Chattopadhyay, Utpal Dasgupta and Uttam Das, eds., Point: Journal of the Department of Mathematics, no. 1, pp. 1–12. Sree Chaitanya College, Habra, 2005.
28. **Souradyuti Paul**, Bart Preneel. *Near Optimal Algorithms for Solving Differential Equations of Addition with Batch Queries.* In Subhamoy Maitra, C. E. Veni Madhavan and Ramarathnam Venkatesan, eds., Indocrypt 2005, LNCS 3797, pp. 90–103. Springer, 2005. doi:10.1007/11596219_8
29. **Souradyuti Paul**, Bart Preneel. *Solving Systems of Differential Equations of Addition.* In Colin Boyd and Juan Manuel González Nieto, eds., ACISP 2005, LNCS 3574, pp. 75–88. Springer, 2005. doi:10.1007/11506157_7
30. **Souradyuti Paul**, Bart Preneel. *A New Weakness in the RC4 Keystream Generator and an Approach to Improve the Security of the Cipher.* In Bimal K. Roy and Willi Meier, eds., FSE 2004, LNCS 3017, pp. 245–259. Springer, 2004. doi:10.1007/978-3-540-25937-4_16
31. **Souradyuti Paul**, Bart Preneel. *Analysis of Non-fortuitous Predictive States of the RC4 Keystream Generator.* In Thomas Johansson and Subhamoy Maitra, eds., Indocrypt 2003, LNCS 2904, pp. 52–67. Springer, 2003. doi:10.1007/978-3-540-24582-7_4

IACR EPRINT

1. Gautham Sekar, **Souradyuti Paul**, Bart Preneel. *Weaknesses in the Pseudorandom Bit Generation Algorithms of the Stream Ciphers TPypy and TPy.* Cryptology ePrint Archive, Report 2007/075, 2007. eprint.iacr.org/2007/075

COURSES TAUGHT

A full list of courses taught is available on request.

THESIS SUPERVISION

Ph.D.

Vijay Shankar Tiwari, IIT Bhilai. Privacy in Blockchain. Jul 2025 – present

Abu Talha, IIT Bhilai. Privacy-preserving Blockchain. Jul 2024 – present

Kolichala Rajashekar, IIT Bhilai. Machine Learning for Resource Provisioning in Stationary and Non-Stationary Edge Computing. Jointly supervised with Dr Subhajit Sidhanta. Jul 2019 – 2025

Suyash Kandele, IIT Bhilai. Design and Analysis of Message-locked Encryptions and Its Variants. Jul 2015 – 2020

Ananya Shrivastava, IIT Gandhinagar. Fair Multiparty Computation using Blockchain. Jul 2014 – 2021

M.Tech.

Bhakti Dhorajiya, M.Tech. (CSE), IIT Bhilai. Improving the Efficiency of E-voting Protocols. 2023 – present

Ruchit Saxena, M.Tech. (CSE), IIT Bhilai. Security Analysis of the Unified Payments Interface (UPI) System in India. 2024

Arti Dhiman, M.Tech. (CSE), IIT Bhilai. Applications of Blockchain in Trust-intensive Environments. 2023

Manish Kumar, M.Tech. (Cryptography), Indian Statistical Institute. Decentralized Marketplace for NFTs. 2022

Saibaba Kothakopu, M.Tech. (Cryptography), Indian Statistical Institute. Oblivious and Fair Data Trading Protocol using Blockchain. 2022

Sarbajit Ghosh, M.Tech. (Cryptography), Indian Statistical Institute. Design of Blockchain-based E-voting Protocols. 2021

Vuppala Manish, M.Tech. (CSE), IIT Bhilai. Implementation of Blockchain-based E-voting Protocols. 2020 – 21

Mohammad Sumair, M.Tech. (CSE), IIT Bhilai. Blockchain-based Trading Protocols. 2019 – 20

Yash Kumar, M.Tech. (CSE), IIT Bhilai. Decoy Routing Algorithms. 2018 – 19

Babita Shakya, Master's student, IIT Gandhinagar. Lattice-based Cryptography. 2016 – 17

Gorka Munduate, Erasmus student at KU Leuven, University of UPV/EHU, Basque Country, Spain. Cryptanalysis of the Stream Cipher RC4A. 2004 – 05

Gautham Sekar, visitor to ESAT, KU Leuven; Master's student, Birla Institute of Technology, Pilani, India. Cryptanalysis of the Stream Cipher Py. The thesis won the Dr. Ranjit Singh Chauhan Undergraduate Research Award for 2006–2007. Jul – Dec 2005

B.Tech.

Amit Chandra (IIT Kanpur, 2008) • Parth Sane (IIT Gandhinagar, 2014) • Arjun Singh Khushawa (IIT Bhilai, 2020)

INTERNSHIPS SUPERVISED (SELECTED)

Samir Vyas and Karma Patel (IIT Gandhinagar), Abhishek Tiwari (IIT Dhanbad), all in 2015.

ATOS International IT Challenge 2017 — Rajat Goel, Ankur Singh and Ayaz Lakhani (IIT Gandhinagar, 2017), *Blockchains for Organ Transfer.* Short-listed among 17 proposals chosen from 77 submissions across 19 countries; of 21 Indian submissions, the IIT Gandhinagar team was the only one selected.

SPONSORED PROJECTS

As Principal Investigator

FinTech Security with (or without) Blockchain 2025 – 2030
Sponsor: MeitY (through the ISEA-3 programme). Budget: INR 6,00,00,000 – 9,00,00,000.

Climate and Energy Centre of Excellence 2025 – 2026
Sponsor: UNICEF. Budget: INR 27,00,000.

Water ATM 2025 – 2026
Sponsor: Chhattisgarh Administration. Budget: INR 25,00,000.

Dantewada Development Project 2024 – 2026
Sponsor: District Mineral Fund, Dantewada. Budget: INR 59,00,000.

P2P Online Marketplace 2023 – 2026
Sponsor: Sapio Global Analytics. Budget: INR 55,20,000.

P2P Online Marketplace 2023 – 2026
Sponsor: IBITF. Budget: INR 8,60,000.

Solar Energy Trading Platform 2022 – 2025
Sponsor: DST. Budget: INR 18,94,560.

GI Tags
Sponsor: IBITF. Budget: INR 84,50,000.

As Co-Principal Investigator

Vidya Samiksha Kendra 2024 – 2027
Sponsor: Education Ministry, Government of Chhattisgarh. Budget: INR 4,69,00,000.

As Team Member

SHA-3 (Contract G-3-00334) 2007 – 2012
Sponsor: Department of Commerce, Government of the USA. Objective: design of a cryptographically strong hash function for the US Government. Role: evaluation and cryptanalysis. 64 teams worldwide; budget of several million dollars (exact amount undisclosed). csrc.nist.gov

ECRYPT-eSTREAM (Contract IST-2002-507932) 2004 – 2008
Sponsor: European Commission. Objective: design of stream ciphers suitable for widespread adoption. Role: cryptanalysis. 32 major European universities; budget of several million euros (exact amount undisclosed). ecrypt.eu.org

SELECTED TALKS

Invited

- *Blockchains: Truth vs. Hype.* Keynote talk, BITCON 2019, Bhilai Institute of Technology, Durg, Chhattisgarh, India.
- *Lottery on the Internet: A Fairy Tale?* 12th National Frontiers of Engineering, IIT Guwahati, Assam, India.
- *Password Cracking and Countermeasures.* National Workshop on Network, Network Simulation & Information Security, Gujarat, India, 2014.
- *How Cryptography Has Shaped Human Civilization: From Julius Caesar to Edward Snowden.* Cybersecurity Workshop, IIT Gandhinagar, 2014.
- *Modes of Operation in Light-weight Symmetric Crypto.* Seminar at George Mason University, USA, October 2011.
- *How to Make the Py-family of Stream Ciphers Secure.* Center for Information Security Technologies (CIST), Korea University, August 2007.
- *Security of Hash Functions.* ComSec Research Seminar, University of Waterloo, Canada, November 16, 2005.
- *Differential Equations of Addition: Theory and Practice.* Centre for Applied Cryptographic Research (CACR), University of Waterloo, Canada, November 10, 2005.
- *Pseudorandom Bit Generators (PRBGs) and Stream Ciphers Based on Random Shuffle.* Centre for Applied Cryptographic Research (CACR), University of Waterloo, Canada, October 20, 2005.
- *Weaknesses in the RC4-like Ciphers, Parts I and II.* Applied Statistics Unit, Indian Statistical Institute, December 15 and 22, 2003.

Other

- *NIST's Plan for Handling Security Parameters.* 1st SHA-3 Candidate Conference, Leuven, Belgium, 2009. Transcript at csrc.nist.gov

PROFESSIONAL SERVICE (SELECTED)

Selection Committees

- Smart India Hackathon, 2019
- Chhattisgarh: Blockchain for e-Governance Grand Challenge, 2018
- SHA-3 winner selection — 1 from 5 algorithms, 2010–2012
- SHA-3 finalists selection — 5 from 14 algorithms, 2009–2010
- SHA-3 semi-finalists selection — 14 from 51 algorithms, 2008–2009
- SHA-3 first-round selection — 51 from 64 submitted algorithms, 2007–2008

Technical Programme Committees

- ISEA-ISAP 2026
- Indocrypt 2026
- Indocrypt 2025
- Secure Knowledge Management (SKM) 2019, Goa
- International Conference on Blockchain Technologies (IC-BCT) 2019, Mumbai

- 20th ICISC 2017, Seoul, Korea
- ISEA Asia Security and Privacy 2017, Gujarat, India
- 18th ICISC 2015, Seoul, Korea
- 10th 3PGCIC 2015, Krakow, Poland
- 16th SRF-ICDCN 2015, Goa, India
- NWNSIS 2014, Gujarat, India (advisory committee)
- 17th ICISC 2014, Seoul, Korea
- 3rd SHA-3 Candidate Conference 2012, Washington DC, USA
- ECRYPT-II Hash Workshop 2011, Tallinn, Estonia
- 2nd SHA-3 Candidate Conference 2011, California, USA
- 1st SHA-3 Candidate Conference 2009, Leuven, Belgium

Review Services (selected)

Journal of Cryptology; Crypto; Eurocrypt; Asiacrypt; Discrete Mathematics; IEEE Transactions on Information Theory.

ADMINISTRATIVE SERVICE

Institute Responsibilities

Faculty-in-charge, Campus Safety, IIT Bhilai	2023 – present
Faculty-in-charge, Website Content Management, IIT Bhilai	2018 – 19
Faculty-in-charge, Newsletter & Annual Reports, IIT Bhilai	2017 – 19

Departmental Responsibilities

Associate Head, Computer Science and Engineering, IIT Bhilai	2023 – present
Convenor, DPGC (EECS), IIT Bhilai	2018 – 2021
Faculty Advisor, M.Tech. 2017 (CSE), IIT Bhilai	2017 – 18
Faculty Advisor, B.Tech. 2017 (CSE), IIT Bhilai	2017 – 18
Convenor, DUGC (CSE), IIT Bhilai	2017 – 18
Convenor, DPGC (CSE), IIT Bhilai	2017 – 18
Convenor, Ph.D. Admission, IIT Gandhinagar	2014 – 16
Coordinator, B.Tech./M.Tech./Ph.D. projects, IIT Gandhinagar	2014 – 16
Coordinator, Website Development for CSE, IIT Gandhinagar	2014 – 16

PERSONAL DETAILS

Citizenship: Indian • **Residence:** Durg, Chhattisgarh, India
Languages: Bengali (mother tongue), English (fluent), Hindi (fluent)

REFEREES

Available on request.