Dr Souradyuti Paul **November 25, 2025**

Address

Department of Computer Science
Office # 405B, ED1
IIT Bhilai
PIN 491002, Chhattisgarh, India.

Mob: +(+91) 823 805 0231
email: souradyuti@iitbhilai.com
web: https://souradyutip.github.io

Research Interests Cryptographic modes and multiparty protocols; Blockchain and Cryptocurrency; Anonymity and Privacy; Network Security

Professional Experience

Associate professor, Computer science and engineering, IIT Bhilai, Oct. 2017 – present

Assistant professor, Computer science and engineering, IIT Gandhinagar, July 2014 – Oct. 2017

Postdoctoral researcher, Combinatorics & Optimization Dept., & David R. Cheriton school of computer science, Univ. of Waterloo, Canada, 2012 – 2014
Mentor: Profs. Alfred Menezes and Douglas Stinson.

Guest researcher, Computer Security Div., National Inst. of Standards and Technology (NIST), USA, 2008 – 2012
Project: Evaluation of US Govt. 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 Honors

Nominated to serve on the steering committee for nationwide ACM India Cyber-security Initiative, 2021.

Nominated to lead multiple Indian initiatives (organized by the Bureau of Indian Standards) for standardizing Blockchain-based applications under various ISO projects, 2019.

Invited to be a judge at *Smart India Hackathon* (*certificate from Ministry of Education for exceptional contribution*), 2019.

Excellence in research fellowship, IIT Gandhinagar, 2014.

Served on the evaluation committee for the US Govt. Cryptographic hash function standard *SHA-3*, 2008 – 2012.

Ranked 111 out of 100,000+ (99.9th percentile) in West Bengal Joint Entrance Examination 1994 (WB-JEE 1994).

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

Publications in Fully Peer-reviewed Journals, Book-series and Conferences (International)

[1] Souradyuti Paul, Devansh Shrivastava. **Energy Trading Using Blockchain at IIT Bhilai Campus.** *ISEA Annual Magazine 2026 (accepted).* To be published.

[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, pages 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, pages 63 – 85.* doi:10.1007/978-3-031-63992-0_5

[5] Kolichala Rajashekar, Sushanta Karmakar, Souradyuti Paul, and 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*, pages 286–287. ACM, 2023. doi:10.1145/3571306.3571417

[6] Arti Dhiman, Souradyuti Paul. **Blockchain-based E-voting: A Status Update.** *India Internet Governance Forum 2023 (IIGF 2023).* https://www.pib.gov.in/PressReleaseIframePage.aspx?PRID=1982217

[7] Kolichala Rajashekar, Souradyuti Paul, Sushanta Karmakar and 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*, pages 1310–1311. IEEE, 2022. doi:10.1109/ICDCS54860.2022.00144

[8] Souradyuti Paul and Ananya Shrivastava. **Efficient Fair Multiparty Protocols using Blockchain and Trusted Hardware.** In Peter Schwabe and Nicolas Thériault, editors, *6th International Conference on Cryptology and Information Security in Latin America, Latincrypt*, vol. 11774 of *Lecture Notes in Computer Science*, pages 301-320. Springer, Cham. 2019. doi:10.1007/978-3-030-30530-7_15

[9] Suyash Kandele and Souradyuti Paul. **Key Assignment Scheme with Authenticated Encryption**. *IACR Transactions of Symmetric Cryptology*, vol. 2018, no. 4, pp. 150-196. 2018. doi:10.13154/tosc.v2018.i4.150-196

[10] Souradyuti Paul and Ananya Shrivastava. **Robust Multiparty Computation with Faster Verification Time**. In Willy Susilo and Guomin Yang, editors, *Information Security and Privacy - 23rd Australasian Conference (ACISP) 2018*, vol. 10946 of *Lecture Notes in Computer Science*, pages 114-131. Springer, Cham. 2018. doi:10.1007/978-3-319-93638-3_8

[11] Suyash Kandele and Souradyuti Paul. **Message-Locked Encryption with File Update**. In Bart Preneel and Frederik Vercauteren, editors, *Applied Cryptography and Network Security - 16th International Conference (ACNS) 2018*, vol. 10892 of *Lecture Notes in Computer Science*, pages 678–695. Springer, Cham. 2018.
doi:10.1007/978-3-319-93387-0_35

[12] Indra Deep Mastan and Souradyuti Paul. **A New Approach to Deanonymization of Unreachable Bitcoin Nodes**. In Srđan Čapkun and Sherman S. M. Chow, editors, *Cryptography and Network Security (CANS) 2017*, vol. 11261 of *Lecture Notes in Computer Science*, pages 277–298. Springer, Cham. 2017.
doi:10.1007/978-3-030-02641-7_13

[13] Sudhakar Kumawat and Souradyuti Paul. **A New Constant-size Accountable Ring Signature Without Random Oracles**. In Xiaofeng Chen and Moti Yung, editors, *Inscrypt 2017*, vol. 10726 of *Lecture Notes in Computer Science*, pages 157–179. Springer, Cham. 2017.
doi:10.1007/978-3-319-75160-3_11

[14] Dustin Moody, Souradyuti Paul, and Daniel Smith-Tone. **Indifferentiaility Security of FWP: Breaking the Birthday Barrier**. *Journal of Mathematical Cryptology*, vol. 10, no. 2, pp. 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.Improved indifferentiability security bound for the JH mode.** *Design, Codes and Cryptography 79(2): 237-259 (2016).*
doi:10.1007/s10623-015-0047-9

[16] 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 (2016)*
doi:10.1515/jmc-2014-0044

[17] Souradyuti Paul, Ekawat Homsirikamol, and Kris Gaj. **A Novel Permutation-based Hash Mode of Operation FP and the Hash Function SAMOSA.** In Steven Galbraith, Mridul Nandi, editors, *Indocrypt 2012,* vol. 7668 of *Lecture Notes in Computer Science*, pages 514 – 532. Springer, 2012.
doi:10.1007/978-3-642-34931-7_29

[18] Dustin Moody, Souradyuti Paul, and Daniel Smith-Tone. **Improved Indifferentiability Security Bound for the JH Mode (Extended Abstract)**. *3rd SHA-3 Candidate Conference*, 2012.
https://www.nist.gov/news-events/events/2012/03/third-sha-3-candidate-conference

[19] Shu-jen Chang, Ray Perlner, William Burr, Meltem Sönmez Turan, John M. Kelsey, Souradyuti Paul, and Lawrence E. Bassham. **Third-Round Report of the SHA-3 Cryptographic Hash Algorithm Competition**. *NIST IR*, vol. 7896. Department Of Commerce, Govt. of US, 2012.
doi: 10.6028/NIST.IR.7896

[20] Meltem Sönmez Turan, Ray Perlner, Lawrence E. Bassham, William Burr, Donghoon Chang, Shu-jen Chang, Morris J. Dworkin, John M. Kelsey, Souradyuti Paul, and Rene Peralta. **Status Report on the Second Round of the SHA-3 Cryptographic Hash Algorithm Competition**. *NIST IR*, vol. 7764. Department Of Commerce, Govt. of US, 2011.
doi: 10.6028/NIST.IR.7764

[21] Mridul Nandi and Souradyuti Paul. **Speeding up the wide-pipe: Secure and fast hashing.** In Guang Gong and Kishan Chand Gupta, editors, *Indocrypt 2010*, vol. 6498 of *Lecture Notes in Computer Science*, pages 144–162. Springer, 2010.
doi:10.1007/978-3-642-17401-8_12

[22] Andrew Regenscheid, Ray Perlner, Shu jen Chang, John Kelsey, Mridul Nandi, and Souradyuti Paul. **Status Report on the First Round of the SHA-3 Cryptographic Hash Algorithm Competition**. *NIST IR*, vol. 7620. Department Of Commerce, Govt. of US, 2009.
doi:10.6028/NIST.IR.7620

[23] Gautham Sekar, Souradyuti Paul, and 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, editors, *WEWoRC 2007*, volume 4945 of *Lecture Notes in Computer Science*, pages 127–141. Springer, 2007.
doi:10.1007/978-3-540-88353-1_11

[24] Gautham Sekar, Souradyuti Paul, and 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, editors, *ISC 2007*, volume 4779 of *Lecture Notes in Computer Science*, pages 249–262. Springer, 2007.
doi:10.1007/978-3-540-75496-1_17

[25] Gautham Sekar, Souradyuti Paul, and 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, editors, *Indocrypt 2007*, volume 4859 of *Lecture Notes in Computer Science*, pages 58–72. Springer, 2007.
doi:10.1007/978-3-540-77026-8_6

[26] Souradyuti Paul and Bart Preneel. **On the (In)security of Stream Ciphers Based on Arrays and Modular Addition**. In Xuejia Lai and Kefei Chen, editors, *Asiacrypt 2006*, volume 4284 of *Lecture Notes in Computer Science*, pages 69–83. Springer, 2006.
doi:10.1007/11935230_5

[27] Souradyuti Paul, Bart Preneel, and Gautham Sekar. **Distinguishing Attacks on the Stream Cipher Py**. In Matthew J. B. Robshaw, editor, *FSE 2006*, volume 4047 of *Lecture Notes in Computer Science*, pages 405–421. Springer, 2006.
doi:10.1007/11799313_26

[28] Souradyuti Paul. **Cryptology: A Mathematician's Quest for Making and Breaking the Code**. In Sanatan Paul, Saroj Kumar Chattopadhyay, Utpal Dasgupta, and Uttam Das, editors, *Point: Journal of Department of Mathematics,* no. 1, pp. 1-12. Sree Chaitanya College, Habra, 2005.

[29] Souradyuti Paul and Bart Preneel. **Near Optimal Algorithms for Solving Differential Equations of Addition with Batch Queries**. In Subhamoy Maitra, C. E. Veni Madhavan, and Ramarathnam Venkatesan, editors, *Indocrypt 2005*, volume 3797 of *Lecture Notes in Computer Science*, pages 90–103. Springer, 2005.
doi:10.1007/11596219_8

[30] Souradyuti Paul and Bart Preneel. **Solving Systems of Differential Equations of Addition**. In Colin Boyd and Juan Manuel González Nieto, editors, *ACISP 2005*, volume 3574 of *Lecture Notes in Computer Science*, pages 75–88. Springer, 2005.
doi:10.1007/11506157_7

[31] Souradyuti Paul and 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, editors, *FSE 2004*, volume 3017 of *Lecture Notes in Computer Science*, pages 245–259. Springer, 2004.
doi:110.1007/978-3-540-25937-4_16

[32] Souradyuti Paul and Bart Preneel. **Analysis of Non-fortuitous Predictive States of the RC4 Keystream Generator**. In Thomas Johansson and Subhamoy Maitra, editors, *Indocrypt 2003*, volume 2904 of *Lecture Notes in Computer Science*, pages 52–67. Springer, 2003.
doi:10.1007/978-3-540-24582-7_4

IACR E-Print

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

Courses Taught

The full list is added to the appendix.

Thesis supervision

PhD

1. Vijay Shankar Tiwari. Title: *Privacy in Blockchain.* IIT Bhilai, Jul 2025 – present.
2. Abu Talha. Title: *Privacy-preserving Blockchain.* IIT Bhilai, Jul 2024 – present.
3. Kolichala Rajashekar. Title: *Machine Learning for Resource Provisioning in Stationary and Non-Stationary Edge Computing.* IIT Bhilai, Jul. 2019 – 2025. (joint supervision with Dr Subhajit Sidhanta)
4. Suyash Kandele. Title: *Design and analysis of Message-locked Encryptions and Its Variants.* IIT Bhilai, Jul. 2015 – 2020.
5. Ananya Shrivastava. Title: *Fair Multiparty Computation using Blockchain.* IIT Gandhinagar, July 2014 – 2021.

MTech

1. Bhakti Dhorajiya. MTech (CSE). IIT Bhilai. Thesis Title: *Improving the Efficiency of E-voting Protocols.* 2023 – present.
2. Ruchit Saxena. MTech (CSE). IIT Bhilai. Thesis Title:*Security Analysis of Unified Payments Interface (UPI) system in India.* IIT Bhilai. *2024.*
3. *Arti Dhiman. MTech (CSE). IIT Bhilai. Thesis Title:* Applications of Blockchain in Trust-intensive Environments. *2023.*
4. *Manish Kumar. MTech (Cryptography). Indian Statistical Institute. Thesis Title:* Decentralized Marketplace for NFTs. *2022.*

5. *Saibaba Kothakopu. MTech (Cryptography). Indian Statistical Institute. Thesis Title:* Oblivious and fair data trading protocol by using Blockchain. *2022.*
6. *Sarbajit Ghosh. MTech (Cryptography). Indian Statistical Institute. Thesis Title:* Design of Blockchain-based E-voting Protocols. *2021.*
7. *Vuppala Manish. MTech (CSE). IIT Bhilai. Thesis Title:* Implementation of Blockchain-based E-voting Protocols. *2020-21.*
8. *Mohammad Sumair. MTech (CSE). IIT Bhilai. Thesis Title:* Blockchain-based Trading Protocols. *2019-20.*
9. *Yash Kumar. MTech (CSE). IIT Bhilai. Thesis Title:* Decoy Routing Algorithms. *2018-19.*
10. *Babita Shakya. Master's student. IIT Gandhinagar. Thesis Title:* Lattice-based cryptography. *2016-17.*
11. *Gorka Munduate. Erasmus student in KU Leuven. University of UPV/EHU, Basque Country, Spain. Thesis Title:* Cryptanalysis of the Stream Cipher RC4A. *2004-05.*
12. *Gautham Sekar. Visitor to ESAT in KU Leuven. Master's student, Birla Institute of Technology, Pilani, India. Thesis Title:* Cryptanalysis of the Stream Cipher Py. *July–Dec 2005. (The thesis won the Dr. Ranjit Singh Chauhan Undergraduate Research Award for the year 2006–2007).*

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

Internship (selected) — Samir Vyas, 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. (This project has made into the short-listed 17 proposals chosen from a pool of 77 submissions from 19 countries. Out of 21 Indian submissions, only IITGN team came out successful.).

Sponsored Projects

As PI

Title: Climate and Energy COE.
Sponsor: UNICEF.
Budget: ₹27,00,000/-.
Duration: 2025 – 2026.

Title: Water ATM.
Sponsor: Chhattisgarh Administration.
Budget: ₹25,00,000/-.
Duration: 2025 – 2026.

Title: FinTech Security with (or without) Blockchain.
Sponsor: MeitY(through the ISEA-3 program).
Budget: Between ₹6,00,00,000/- and ₹9,00,00,000/-.
Duration: 2025 – 2030.

Title: Solar energy trading platform .
Sponsor: DST.
Budget: ₹18,94,560/-.
Duration: 2022 – 2025.

Title: P2P online market place.
Sponsor: Sapio Global Analytics.
Budget: ₹55,20,000.
Duration: 2023 – 2026.

Title: Dantewada Development Project.
Sponsor: District Mineral Fund – Dantewada.
Budget: ₹59,00,000/-.
Duration: 2024 – 2026.

Title: P2P online market place.
Sponsor: IBITF.
Budget: ₹8,60,000/-.
Duration: 2023 – 2026.

Title: GI Tags.
Sponsor: IBITF.
Budget: ₹84,50,000/-
Duration:

As co-PI

Title: Vidya Samiksha Kendra.
Sponsor: Education Ministry, Government of Chhattisgarh.
Budget: ₹4,69,00,000/-
Duration: 2024 – 2027.

As Team Member

Project Name: ECRYPT-eSTREAM.
Sponsor: European Commission.
Contract Number: IST-2002-507932.
Objective: Design of stream ciphers suitable for widespread adoption.
Duration: 2004 – 2008.
Participants: 32 major universities in Europe.
Role: Cryptanalysis.
Budget: Big, approximately several million euros (exact amount undisclosed)
web: http://www.ecrypt.eu.org/ecrypt1/

Project Name: SHA-3.
Sponsor: Department of Commerce, Govt. of USA.
Contract Number: G-3-00334.
Objective: Design of a cryptographically strong hash function for the govt. of US.
Duration: 2007 – 2012.
Participants: 64 teams from across the globe.
Role: Evaluation and Cryptanalysis.
Budget: Big, approximately several million dollars (exact amount undisclosed)
web: http://csrc.nist.gov/groups/ST/hash/sha-3/

Selected Talks

Invited

Blockchains: Truth vs. Hype. BITCON 2019, Bhilai Institute of Technology, Durg, CG, India (**Keynote talk**).

Lottery on the Internet: A Fairy Tale?. 12th Twelveth National Frontiers of Engineering, IIT Guwahati, Assam, India.

Password cracking and countermeasures. National Workshop on Network, Network Simulation & Information Security, 2014, Gujarat, India.

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, US. Oct 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. CACR (Centre for Applied Cryptographic Research), University of Waterloo, Canada. November 10, 2005.

Pseudorandom Bit Generators (PRBGs) and Stream Ciphers Based on Random Shuffle. CACR (Centre for Applied Cryptographic Research), University of Waterloo, Canada. October 20, 2005.

Weaknesses in the RC4-like ciphers – Part II. Applied Statistics Unit, Indian Statistical Institute. December 22, 2003.

Weaknesses in the RC4-like ciphers – Part I. Applied Statistics Unit, Indian Statistical Institute. December 15, 2003.

Other talks

NIST's Plan for Handling Security Parameters. 1st SHA3 candidate Conference, 2009, Leuven, Belgium. Transcript at csrc.nist.gov

Professional Services (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 1st round selection, 51 from 64 submitted algorithms, 2007 – 2008

Technical Program Committees

ISEA-ISAP 2026
Indocrypt 2026
Indocrypt 2025
Secure Knowledge Management (SKM) 2019, Goa
International Conference-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, US
ECRYPT-II Hash Workshop 2011, Tallinn, Estonia
2nd SHA-3 Candidate Conference 2011, California, US
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 Services

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 (CSE), IIT Bhilai (2023 – present) Convenor, DPGC (EECS), IIT Bhilai (2018 - 2021) Faculty advisor, MTech2017 (CSE), IIT Bhilai (2017 - 18) Faculty advisor, BTech2017 (CSE), IIT Bhilai (2017 - 18) Convenor, DUGC (CSE), IIT Bhilai (2017 - 18) Convenor, DPGC (CSE), IIT Bhilai (2017 - 18) Convenor, PhD Admission, IIT Gandhinagar (2014-16) Coordinator, B.Tech/M.Tech/PhD 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	Will be provided on request.