Dr. Souradyuti Paul **March 15, 2019**

Address

Department of EECS
Office # 106, IIT Bhilai
GEC Campus, Sejbahar, Raipur
PIN 492015, Chhattisgarh, India.

Ph: +(+91) 771 255 1300 x 6111
email: souradyuti@iitbhilai.com
web: https://souradyuti.com

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 lead multiple Indian initiatives (organized by *Bureau of Indian Standards*) for standardizing Blockchain-based applications under various projects undertaken by *International Organization for Standardization* (ISO), 2019

Judge at *Smart India Hackathon'19* (certificate from ministry for exceptional contribution)

Keynote speaker at BITCON'19 organized by Bhilai Institute of Technology

Judge at *Chhattisgarh: Blockchain for e-Governance Grand Challenge'18* (organized by CHiPS)

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.

Regional Mathematical Olympiad (RMO) Award for Eastern India Region (Regional rank 16), 1991, presented by Indian Statistical Institute (ISI).

Fellowships

Postdoctoral fellowship from University of Waterloo, 2012 – 2014.

Postdoctoral fellowship from KU Leuven, 2006 – 2008.

Doctoral Scholarship from KU Leuven, 2001 – 2006.

Junior Research Fellowship (JRF) from Indian Statistical Institute, 2001 – 2002.

Publications

Google scholar citation-count = 800

Refereed Journals

[1] 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

[2] 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

[3] Dustin Moody, Souradyuti Paul, and Daniel Smith-Tone. **Improved Indifferentiability Security Bound for the JH Mode**. *Design, Codes and Cryptography*, vol. 79, no. 2, pp. 237-259. Springer, 2016.
doi:10.1007/s10623-015-0047-9

[4] 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

[5] 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

[6] 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

[7] 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.

Book Chapters

[8] 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.

[9] 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.

[10] Indra Deep Mastan and Souradyuti Paul. **De-anonymization of Unreachable Nodes in Bitcoin P2P Network**. 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.

[11] 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.

[12] 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.

[13] Dustin Moody, Souradyuti Paul, and Daniel Smith-Tone. **Improved Indifferentiability Security Bound for the JH Mode (Extended Abstract)**. *3rd SHA-3 Candidate Conference*, 2012.

[14] 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.

[15] 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.

[16] 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.

[17] 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.

[18] 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.

[19] 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.

[20] 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.

[21] 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.

[22] 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.

[23] 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.

IACR E-Print

[24] 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/.

Teaching

Courses

CS554 (Blockchain Technologies). IIT Bhilai, 2018-19-W.

CS254 (Database Management Systems). IIT Bhilai, 2018-19-W.

IC100 (Introduction to Programming-Tutorial). IIT Bhilai, 2018-19-M.

CS202 (Algorithms I). IIT Bhilai, 2018-19-M.

ID1303 (Introduction to Programming). IIT Bhilai, 2017-18-S.

CS2443 (Algorithms). IIT Bhilai, 2017-18-W.

CS2600 (Basics of Number Theoretic Algorithms). IIT Bhilai, 2017-18-M.

CS 606 (Advanced topics in cryptology). IITGN, Summer term, 2016.

CS 431 (Introduction to computer and network security). IITGN, Sem-I, 2015, 2016.

CS 428 (Introduction to applied cryptography). IITGN, Sem-II 2015, 2016, 2017.

FP 101 (Introduction to Engineering). IITGN, Sem-II 2015.

ES 102 (Introduction to computing). IITGN, Sem-I 2014, 2016.

TUTORIALS

Hands-on session on password hashing. National Workshop on Network, Network Simulation & Information Security organized by Dept. of Computer Sc. ISTAR and IEEE Gujarat, 2014.

Overview of Symmetric Cryptology. KU Leuven, Master's Level. July–August in 2004 and 2005.

Overview of Stream Cipher Cryptanalysis. KU Leuven, Master's Level. August–September in 2004 and 2005.

Stream Ciphers in Cryptography. Center for Information Security Technologies (CIST), Korea University. August 2007.

Stream Ciphers in Cryptology-I. KU Leuven, COSIC, BCRYPT (a consortium of European Universities) framework. Dec 2007. Materials at homes.esat.kuleuven.be

Stream Ciphers in Cryptology-II. KU Leuven, COSIC, BCRYPT (a consortium of European Universities) framework, March 2008. Materials at homes.esat.kuleuven.be

Advising

PHD THESES

Suyash Kandele. Tentative title: *Design and analysis of Message-locked Encryptions and Its Variants.* IIT Gandhinagar, Jul. 2015 – present.

Ananya Shrivastava. Tentative title: *Algorithms for Blockchains.* IIT Gandhinagar, July 2014 – present.

MASTER'S THESES

Yash Kumar. M.Tech (CSE). IIT Bhilai. Thesis Title: *Decoy Routing Algorithms.* 2018-19.

Babita Shakya. Master's student. IIT Gandhinagar. Thesis Title: *Lattice-based cryptography.* 2016-17.

Gorka Munduate. Erasmus student in KU Leuven. University of UPV/EHU, Basque Country, Spain. Thesis Title: *Cryptanalysis of the Stream Cipher RC4A.* 2004-05.

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 (The thesis won the Dr. Ranjit Singh Chauhan Undergraduate Research Award for the year 2006–2007).

SHORT PROJECT

PhD students at IIT Gandhinagar: Priodyuti Pradhan, Devendra Mani Tripathi, Diptiben Patel and Vikas Gupta (all in 2014), Ananya Shrivastava (2014 & 2015), Sudhakar Kumawat (2014 & 2015), Indradeep Mastan, Suyash Kandele (all in 2015)

B.Tech students: Amit Chandra (IIT Kanpur, 2008), Parth Sane (IIT Gandhinagar, 2014), Arjun Singh Khushawa (IIT Bhilai, 2020)

B.Tech Interns: 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

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 ï£¡ Part II. Applied Statistics Unit, Indian Statistical Institute. December 22, 2003.

Weaknesses in the RC4-like ciphers ï£¡ 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

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	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
Conference Organization	NMI Workshop on Complexity and Cryptography, 2016, IIT Gandhinagar CoCoA 2016, IIT Gandhinagar Cybersecurity Workshop 2014, IIT Gandhinagar 1st SHA-3 Candidate Conference 2009, Leuven, Belgium 2nd SHA-3 Candidate Conference 2011, California, US 3rd SHA-3 Candidate Conference 2012, Washington DC, US
Memberships	International Association for Cryptologic Research (IACR)
Review Services (selected)	Journal of Cryptology, Crypto, Eurocrypt, Asiacrypt, Discrete Mathematics, IEEE Transactions on Information Theory

Administrative Services

Institute Responsibilities	Faculty-in-charge, Website Content Management, IIT Bhilai (2018 - 19) Faculty-in-charge, Newsletter & Annual Reports, IIT Bhilai (2017 - 19)
Departmental Responsibilities	Convenor, DPGC (EECS), IIT Bhilai (2018 - till date) 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: Raipur, Chhattisgarh, India
Languages: Bengali (mother tongue), English (fluent), Hindi (working) and French (beginner)

Referees Will be provided on request.

(Last updated: March 15, 2019)