



Dr. Suyash Kandeale

🏠 "NEST", 34/6, Nehru Nagar (West), Bhilai, CG 490020, India

🌐 https://suyashkandeale.github.io/Suyash_Kandeale/

✉️ suyashk@iitbhilai.ac.in, sk.11.1992@gmail.com

☎️ (+91) 97546 58975, (+91) 96870 34657

🌐 [linkedin.com/in/suyashkandeale](https://www.linkedin.com/in/suyashkandeale)

Curriculum Vitæ

Objective

I look forward to utilizing my skills and ability in learning the state-of-the-art of cryptography and information security, as well as in solving challenging and innovative research problems in this area. In this way, I like to deeply engage myself in advancing the Internet technologies for the betterment of the society and industry.

Research Interests

Cryptographic Primitives and Protocols; Network Security; Cryptographic Applications in Cloud, IoT, Blockchain, as well as others.

Professional Experience

2020–Now Postdoctoral Researcher

Mentor Prof. Kamalakar Karlapalem

Institute International Institute of Information Technology

Education

2015–20 Doctor of Philosophy in Computer Science and Engineering

Thesis Title Cryptographic Primitives Based on Reverse Decryption

Advisor Dr. Souradyuti Paul

- Institute
- Indian Institute of Technology (IIT) Bhilai
 - Duration: Dec. 2017 – May 2020
 - CPI: [10/10](#)
 - Indian Institute of Technology (IIT) Gandhinagar
 - Duration: July 2015 – Dec. 2017 (continued in IIT Bhilai thereafter)
 - CPI: [9.13/10](#)

2011–15 Bachelor of Technology in Computer Science and Engineering

Institute National Institute of Technology (NIT) Raipur
 CPI [9.23 – Silver Medallist \(with Honours\)](#)

2009-11 HSC (AISSCE 2011) - Equivalent to Class XII

Institute Krishna Public School, Bhilai, Affiliated to Central Board of Secondary Education (CBSE)
 Percentage [85.60% – First Division](#)

1999-2009 SSC (AISSE 2009) - Equivalent to Class X

Institute Krishna Public School, Bhilai, Affiliated to Central Board of Secondary Education (CBSE)
 Percentage [92.00% – First Division](#)

Publications

1. Suyash Kandeale, and Souradyuti Paul, “Key Assignment Scheme with Authenticated Encryption”, *IACR Transactions on Symmetric Cryptology*, vol. 2018, no. 4, pp. 150–196. 2018. This work was presented at *FSE 2019* held in Paris.
 [The 47-page full version is available on *IACR e-print archive* at <https://eprint.iacr.org/2018/1233.pdf>]
 doi: <https://doi.org/10.13154/tosc.v2018.i4.150-196>
2. Suyash Kandeale, 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, Leuven, Belgium, July 2-4, 2018, Proceedings*, vol. 10892 of *Lecture Notes in Computer Science*, pages 678–695. Springer, 2018.
 [The 43-page full version is available on *IACR e-print archive* at <https://eprint.iacr.org/2018/422.pdf>]
 doi: https://doi.org/10.1007/978-3-319-93387-0_35
3. [Preprint] Suyash Kandeale, and Souradyuti Paul, “Efficient AONTs and AONEs Based on Permutations”, The 39-page manuscript has been submitted to *Design, Codes and Cryptography*.

4. Suyash Kandeale, and Veena Anand, “A Novel Square-Expanded-Matrix-Rotation (SEMR) Cryptography Method”, International Journal of Engineering Research and Technology, vol. 4, no. 4, pp. 1366-1378. 2015.
doi: <http://dx.doi.org/10.17577/IJERTV4IS041492>
5. Suyash Kandeale, and Veena Anand, “A Novel Cyclic-Lower-Upper-Rectangular (CLUR) Cryptography Method”, International Journal of Engineering Research and Technology, vol. 3, no. 11, pp. 329-335. 2014.

Awards and Honours

- 2020 Awarded the 1st PhD degree given to a student of any six 3rd Generation IITs. The news (including a feature story) has been published by many prominent media outlets – such as *Patrika* and *Haribhoomi* – in Chhattisgarh state.
- 2017-20 10/10 SPI in all semesters during PhD at IIT Bhilai.
- 2015 Start-Early PhD fellowship by IIT Gandhinagar.
- 2015 Silver Medallist in BTech from NIT Raipur
- 2015 Achieved 99.16th percentile in GATE (Graduate Aptitude Test in Engineering) 2015, organized by Ministry of Human Resources Development (MHRD), Government of India.
- 2011 All India rank 22 (State rank 2) in 10th National Cyber Olympiad conducted by Science Olympiad Foundation (SOF).
- 2007 Awarded the scholarship under National Talent Search Examination, 2007 by National Council of Educational Research and Training (NCERT).

Technical Expertise

Programming C, C++, MATLAB
 Presentation Microsoft PowerPoint, L^AT_EX
 Platform Windows & UNIX
 Database SQL, Microsoft Access

Projects Undertaken at Bachelor's Level

- Major Project **A Novel Square-Expanded-Matrix-Rotation (SEMR) Cryptography Method**
Advisor: Dr. Veena Anand, Assistant Professor, CSE, NIT Raipur.
- Minor Project **A Novel Cyclic-Lower-Upper-Rectangular (CLUR) Cryptography Method**
Advisor: Dr. Veena Anand, Assistant Professor, CSE, NIT Raipur.
- Internship Project **Digital Image Watermarking:** An Image Hiding Application, that hides a Message Image under a Cover Image, Summer Internship, 3rd Year, 2014

Personal Information

Citizenship Indian
Languages Hindi (Mother tongue), English (Fluent)
Hobbies Photography, Gardening, Cooking

Referees

- **Dr. Souradyuti Paul**
Associate Professor, EECS, IIT Bhilai.
E-mail: souradyuti@iitbhillai.ac.in
Phone: (+91) 82380 50231
- **Dr. Dhiman Saha**
Assistant Professor, EECS, IIT Bhilai.
E-mail: dhiman@iitbhillai.ac.in
Phone: (+91) 97335 04768
- **Prof. Kamalakar Karlapalem**
Professor,
IIIT Hyderabad.
E-mail: kamal@iiit.ac.in
Phone: (+91) 40 6653 1000 Ext. 1140
- **Prof. Anirban Dasgupta**
N Rama Rao Chair Professor, CSE,
IIT Gandhinagar.
E-mail: anirbandg@iitgn.ac.in
Phone: (+91) 87585 49267
- **Dr. Manu Awasthi**
Associate Professor, CS, Ashoka University.
E-mail: manu.awasthi@ashoka.edu.in
Phone: (+91) 95364 29395

Declaration

I hereby declare that the aforementioned information is correct and current to the best of my knowledge.

Date August 19, 2020
Place Raipur, Chhattisgarh