# Ashwin Jha


**Contact Information**

R. C. Bose Centre for Cryptology and Security
Indian Statistical Institute Kolkata
203 Barrackpore Trunk Road
Kolkata 700108, India

Email: ashwin_r@isical.ac.in, letterstoashwin@gmail.com
Phone: +91 9163921552


**Research Interests**

- Cryptography
- Computational Complexity

**Current Position**

**Visiting Scientist**, since July 2020

- Centre: R. C. Bose Centre for Cryptology and Security
- Institute: Indian Statistical Institute, Kolkata, India

**Education**

**Doctor of Philosophy in Computer Science**, July 2015 – June 2020

- Dissertation Title: *Provable Security of Symmetric-key Cryptographic Schemes*
- Advisor: Dr. Mridul Nandi
- Institute: Indian Statistical Institute, Kolkata, India

**Master of Technology in Computer Science**, July 2013 – July 2015

- *First Class with Honours* (Aggregate: 78%)
- Dissertation Title: *Cryptanalysis of Iterated Hash and Its Variants*
- Advisor: Dr. Mridul Nandi
- Institute: Indian Statistical Institute, Kolkata, India

**Bachelor of Engineering in Computer**, August 2008 – June 2012

- *First Class* (Aggregate: 67%)
- Final Year Project Title: *Segmented Offline Handwriting Recognition Tool*
- Advisor: Dr. Akshi Kumar
- Institute: Delhi College of Engineering, University of Delhi, Delhi, India

**Higher Secondary**, May 2008

- *First Division* (Aggregate: 81%)
- Board: Central Board of Secondary Education
- Institute: Kendriya Vidyalaya Janakpuri, Delhi, India

**Secondary**, May 2006

- *First Division* (Aggregate: 73.4%)
- Board: Central Board of Secondary Education
- Institute: Kendriya Vidyalaya Janakpuri, Delhi, India

**Research Papers**

- A. Jha and M. Nandi, *Tight Security of Cascaded LRW2.* J. Cryptology 33(3): 1272–1317, 2020. DOI: 10.1007/s00145-020-09347-y
- A. Chakraborti, N. Datta, A. Jha, C. Mancillas-López, M. Nandi and Y. Sasaki *INT-RUP Secure Lightweight Parallel AE Modes.* IACR Trans. Symmetric Cryptol. 2019(4): 81–118, 2019. DOI: 10.13154/tosc.v2019.i4.81-118
- A. Jha, C. Mancillas-López, M. Nandi and S. Sen Gupta *On Random Read Access in OCB.* IEEE Trans. Information Theory 65(12): 8325–8344, 2019. DOI: 10.1109/TIT.2019.2925613
- A. Jha and M. Nandi, *On Rate-1 and Beyond-the-Birthday Bound Secure Online Ciphers using Tweakable Block Ciphers.* Cryptography and Communications 10(5): 731–753, 2018. DOI: 10.1007/s12095-017-0275-0
- A. Jha, E. List, K. Minematsu, S. Mishra and M. Nandi, *XHX - A Framework for Optimally Secure Tweakable Block Ciphers from Classical Block Ciphers and Universal Hashing.* LATINCRYPT, 2017:207–227, 2017. DOI: 10.1007/978-3-030-25283-0_12

- A. Dutta, A. Jha and M. Nandi, *A New Look at Counters: Don't Run Like Marathon in a Hundred Meter Race*. IEEE Trans. Computers 66(11):1851–1864, 2017. DOI: 10.1109/TC.2017.2710125
- A. Dutta, A. Jha and M. Nandi, *Tight Security Analysis of EHtM MAC*. IACR Trans. Symmetric Cryptol. 2017(3):130–150, 2017. DOI: 10.13154/tosc.v2017.i3.130-150
- A. Jha, A. Mandal and M. Nandi, *On The Exact Security of Message Authentication Using Pseudorandom Functions*. IACR Trans. Symmetric Cryptol. 2017(1):427–448, 2017. DOI: 10.13154/tosc.v2017.i1.427-448
- A. Jha and M. Nandi, *Revisiting Structure Graphs: Applications to CBC-MAC and EMAC*. J. Mathematical Cryptology. 10(3–4):157–180, 2016. DOI: 10.1515/jmc-2016-0030
- A more comprehensive list is available on DBLP.

## Teaching

**Advanced Cryptology**, Autumn 2020
- Course: M. Tech. (Cryptology and Security)
- Role: Co-instructor
- Institute: Indian Statistical Institute, Kolkata

**Cryptology**, Autumn 2018
- Course: M. Tech. (Computer Science) B2
- Role: Co-instructor
- Institute: Indian Statistical Institute, Kolkata

**Computing Systems I (OS & Architecture)**, Autumn 2018
- Course: M. Tech. (Cryptology and Security) A2
- Role: Teaching Assistant
- Institute: Indian Statistical Institute, Kolkata

**Data and File Structures Laboratory**, Autumn 2015
- Course: M. Tech. (Computer Science) A2
- Role: Teaching Assistant
- Institute: Indian Statistical Institute, Kolkata

## Industrial and Open Source Experience

**Google Summer of Code 2014 Intern**, April 2014 – August 2014
- Organization: Eclipse Foundation
- Supervisor: Marcel Bruch
- Summary: Developed a centralized logging framework for the Eclipse IDE platform.

**Software Engineer**, July 2012 – July 2013
- Organization: Algoworks Technologies
- Summary: Worked in the Android Application Development Team.

**Software Intern**, May 2011 – July 2011
- Organization: ESQ Management Solutions Inc.
- Summary: Studied the ESQ ATM and POS Management Products and built test cases for ATM and POS Analytics.

## Technical Skills

- Programming Languages: C, C++, Java
- Markup Languages: LaTeX, HTML
- Operating Systems: Linux, Windows
- Github profile: migfi