Ashwin Jha

Updated on February 24, 2021

Office: CISPA – Helmholtz Center for Information Security
Stuhlsatzenhaus 5, 66123 Saarbrücken, Germany

Web: ashwin-jha.github.io

Email: letterstoashwin@gmail.com

Phone: +49 681 87083 2218

Research Interests

My research interests are primarily in symmetric-key cryptography, with a special focus on the *design and analysis of symmetric-key modes of operation.*

Current Position

Postdoctoral Researcher January, 2021 – present
CISPA – Helmholtz Center for Information Security Saarbrücken, Germany
Host: Dr. Benoît Cogliati

Education

Doctor of Philosophy in Computer Science July, 2015 – June, 2020
Indian Statistical Institute Kolkata, India
Dissertation: Provable Security of Symmetric-key Cryptographic Schemes
Advisor: Prof. Mridul Nandi

Master of Technology in Computer Science July 2013 – July 2015
Indian Statistical Institute Kolkata, India
Dissertation: Cryptanalysis of Iterated Hash and Its Variants
First class *with Honours* (Aggregate: 78%), *Best Dissertation Award*
Advisor: Prof. Mridul Nandi

Bachelor of Engineering in Computer August 2008 – June 2012
Delhi College of Engineering, University of Delhi Delhi, India
First class (Aggregate: 67%)

Research Experience

Postdoctoral Researcher January, 2021 – present
CISPA – Helmholtz Center for Information Security Saarbrücken, Germany
Working on the design and analysis of symmetric-key modes of operations.

Visiting Scientist July 2020 – December 2020
R. C. Bose Centre for Cryptology and Security, Kolkata, India
Indian Statistical Institute
Worked on the design and analysis of lightweight authenticated encryption mode.

Research Intern January 2018 – March 2018
Fujitsu Laboratories of America Sunnyvale, USA
Worked on the cryptanalysis of pseudorandom functions using quantum query access.

Research Intern August 2017 – October 2017
NTT Secure Platform Laboratories Tokyo, Japan
Worked on the provable security of tweakable block cipher based modes of operation.

Research Fellow July 2015 – June 2020
Applied Statistics Unit, Indian Statistical Institute Kolkata, India
Worked on the provable security analysis of symmetric-key modes of operations.

Publications*

B. Cogliati, A. Jha and M. Nandi: *How to Build Optimally Secure PRFs Using Block Ciphers.* IACR ASIACRYPT 2020(Part I):754–784, 2020.

A. Jha and M. Nandi: *Tight Security of Cascaded LRW2.* J. Cryptology 33(3): 1272–1317, 2020.

B. Chakraborty, A. Jha and M. Nandi: *On the Security of Sponge-type Authenticated Encryption Modes.* IACR Trans. Symmetric Cryptol. 2020(2): 93–119, 2020.

A. Chakraborti, N. Datta, A. Jha, S. Mitragotri and M. Nandi: *From Combined to Hybrid: Making Feedback-based AE even Smaller.* IACR Trans. Symmetric Cryptol. 2020(S1): 417–445, 2020.

A. Chakraborti, N. Datta, A. Jha, C. Mancillas-López, M. Nandi and Y. Sasaki: *ESTATE: A Lightweight and Low Energy Authenticated Encryption Mode.* IACR Trans. Symmetric Cryptol. 2020(S1): 350–389, 2020.

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.

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.

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.

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.

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.

A. Dutta, A. Jha and M. Nandi: *Tight Security Analysis of EHtM MAC.* IACR Trans. Symmetric Cryptol. 2017(3): 130–150, 2017.

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.

A. Jha and M. Nandi: *Revisiting Structure Graphs: Applications to CBC-MAC and EMAC.* J. Mathematical Cryptology. 10(3–4): 157–180, 2016.

* A more comprehensive list is available on DBLP.

Talks and Tutorials

How to Build Optimally Secure PRFs Using Block Ciphers
IACR ASIACRYPT 2020 (held in online mode)

On the Security of Sponge-type Authenticated Encryption Modes
IACR FSE 2020 (held in online mode)

From Combined to Hybrid: Making Feedback-based AE even Smaller
IACR FSE 2020 (held in online mode)

ESTATE: A Lightweight and Low Energy Authenticated Encryption Mode
IACR FSE 2020 (held in online mode)

Towards an Improved Bound on CBC Collision Probability and Its Applications
India Crypto Meet 2020 (held in online mode)

Hash Functions and Message Authentication Codes
ISI Summer Internship in Cryptology 2018 — Kolkata, India

On The Exact Security of Message Authentication Using Pseudorandom Functions
FSE 2017 — Tokyo, Japan

A New Look at Counters: Don't Run Like Marathon in a Hundred Meter Race
DIAC 2016 — Nagoya, Japan

Teaching Experience

Co-instructor — Advanced Cryptology [M. Tech. (CrS) III]
Indian Statistical Institute Kolkata, India — Autumn 2020

Co-instructor — Cryptology [M. Tech. (CS) III]
Indian Statistical Institute, Kolkata, India — Autumn 2018

Teaching Assistant — Computing Systems I [M. Tech. (CrS) I]
Indian Statistical Institute, Kolkata, India — Autumn 2018

Teaching Assistant — Data and File Structures Lab. [M. Tech. (CS) I]
Indian Statistical Institute, Kolkata, India — Autumn 2015

Reviewing Activities

Journal Reviews: Springer DCC, IET Information Security, IEICE Transactions, The Computer Journal

External Reviewing: CRYPTO, EUROCRYPT, ASIACRYPT, FSE, INDOCRYPT, CANS, IEEE IT

Industry Experience

Google Summer of Code 2014 Intern — April 2014 – August 2017
Eclipse Foundation
Developed a centralized logging framework for the Eclipse IDE platform.

Software Engineer — June 2012 – July 2013
Algoworks Technologies — Noida, India
Worked in the Android applications development team.

Software Intern — May 2011 – July 2011
ESQ Management Solutions Inc. — Noida, India
Built test cases for ATM and POS analytics.

Fellowships and Awards

Doctoral Research Fellowship (ISI Kolkata) — 2015–2020
Student Travel Grant (IACR) — FSE (2017, 2020)
Suniti Kumar Pal Gold Medal (ISI Kolkata) — 2015
Google Summer of Code Fellowship (Google) — 2014

Skills

Programming: C, C++, Java

Markup: LaTeX, HTML

Languages: English, Hindi, Maithili

References

Prof. Mridul Nandi mridul@isical.ac.in
Indian Statistical Institute Kolkata, India

Dr. Kan Yasuda yasuda.kan@lab.ntt.co.jp
NTT Secure Platform Laboratories Tokyo, Japan

Prof. Shay Gueron shay@math.haifa.ac.il
University of Haifa Haifa, Israel

Dr. Yu Sasaki sasaki.yu@lab.ntt.co.jp
NTT Secure Platform Laboratories Tokyo, Japan

Prof. Guruprasad Kar gkar@isical.ac.in
Indian Statistical Institute Kolkata, India

Dr. Arijit Bishnu arijit@isical.ac.in
Indian Statistical Institute Kolkata, India