Ashwin Jha

Updated on January 4, 2024

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

Nationality: India
Residency: Germany
Date of Birth: 21 July, 1991

Web: ashwin-jha.github.io
Email: letterstoashwin@gmail.com
Phone: (+49) 1517 510 3739

Research Interests

Primarily in cryptography, with a special focus on the *provable security of symmetric-key schemes* both in classical and quantum settings.

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

Jump.Start Early Career Researcher January, 2024 onwards
Horst-Görtz Institute for IT Security
Ruhr-Universität Bochum Bochum, Germany
Fortifying symmetric cryptography against advanced adversaries.

Postdoctoral Researcher January, 2021 – December 2023
CISPA Helmholtz Center for Information Security Saarbrücken, Germany
Design and analysis of symmetric-key modes of operations.

Visiting Scientist July 2020 – December 2020
R. C. Bose Centre for Cryptology and Security
Indian Statistical Institute Kolkata, India
Design and analysis of lightweight authenticated encryption modes.

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

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

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

Teaching/Mentoring Experience

Master's Thesis Supervision — Summer Internship [M. Tech. (CrS) IV]
Indian Statistical Institute Kolkata, India — Spring 2022
(work carried out at CISPA Helmholtz Center for Information Security, Germany)

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

Seminars and Workshops

Dagstuhl Seminar on Symmetric Cryptography — 2022
Lorentz Center Workshop on Flexible Symmetric Cryptography — 2018
Asian Workshop on Symmetric Key Cryptography — 2015, 2016, 2018

Reviewing Services

Editorial Board Membership: FSE 2024/ToSC 2023–2024, CANS 2023
FSE 2023/ToSC 2022–2023, CANS 2022
Journal Reviewing: Springer DCC, IET Information Security, IEEE IT
External Reviewing: CRYPTO, EUROCRYPT, ASIACRYPT, FSE

Fellowships and Awards

Jump.Start Fellowship (CASA, RUB) — 2023
Winner of Lightweight Crypto Challenge (DSCI and Govt. of India) — 2021
Suniti Kumar Pal Gold Medal (ISI Kolkata) — 2015
Google Summer of Code Fellowship (Google) — 2014

Industry Experience

Google Summer of Code 2014 Intern — April 2014 – August 2017
Eclipse Foundation

Software Engineer — June 2012 – July 2013
Algoworks Technologies — Noida, India

Software Intern — May 2011 – July 2011
ESQ Management Solutions Inc. — Noida, India

References

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

Dr. Benoît Cogliati — benoit.cogliati@gmail.com
Thales DIS France SAS — Meudon, France

Dr. Bart Mennink — b.mennink@cs.ru.nl
Radboud University — Nijmegen, Netherlands

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

Dr. Yu Sasaki yu.sasaki.sk@hco.ntt.co.jp
NTT Secure Platform Laboratories Tokyo, Japan
Prof. Shay Gueron shay@math.haifa.ac.il
University of Haifa Haifa, Israel

Publications*

N. Balachandran, A. Jha, M. Nandi, S. Pal: *Revisiting Randomness Extraction and Key Derivation Using the CBC and Cascade Modes.* IACR Trans. Symmetric Cryptol. 2023(4), 391–419, 2023.

B. Cogliati, J. Ethan, A. Jha, S. Kanti Saha: *On Large Tweaks in Tweakable Even-Mansour with Linear Tweak and Key Mixing.* IACR Trans. Symmetric Cryptol. 2023(4): 330–364, 2023.

R. Bhaumik, B. Cogliati, J. Ethan, A. Jha: *On Quantum Secure Compressing Pseudorandom Functions.* IACR ASIACRYPT 2023(Part III): 34–66, 2023.

A. Gunsing, R. Bhaumik, A. Jha, B. Mennink, Y. Shen: *Revisiting the Indifferentiability of the Sum of Permutations.* IACR CRYPTO 2023(Part III): 628–660, 2023.

B. Cogliati, J. Ethan, A. Jha: *Subverting Telegram's End-to-End Encryption.* IACR Trans. Symmetric Cryptol. 2023(1): 5–40, 2023.

S. Chattopadhyay, A. Jha, M. Nandi: *Towards Tight Security Bounds for OMAC, XCBC and TMAC.* IACR ASIACRYPT 2022(Part I): 348–378, 2022.

A. Jha, M. Nandi: *A Survey on Applications of H-Technique: Revisiting Security Analysis of PRP and PRF.* Entropy 24(4): 462, 2022.

S. Chattopadhyay, A. Jha, M. Nandi: *Fine-Tuning the ISO/IEC Standard LightMAC.* IACR ASIACRYPT 2021(Part III): 490–519, 2021.

S. Gueron, A. Jha, M. Nandi: *Revisiting the Security of COMET Authenticated Encryption Scheme.* INDOCRYPT 2021: 3–25, 2021.

A. Chakraborti, N. Datta, A. Jha, C. Mancillas-López, M. Nandi: *tHyENA: Making HyENA Even Smaller.* INDOCRYPT 2021: 26–48, 2021

A. Chakraborti, N. Datta, A. Jha, C. Mancillas-López, M. Nandi, Y. Sasaki: *Elastic-Tweak: A Framework for Short Tweak Tweakable Block Cipher.* INDOCRYPT 2021: 114-137, 2021.

A. Chakraborti, N. Datta, A. Jha, C. Mancillas-López, M. Nandi: *Light-OCB: Parallel Lightweight Authenticated Cipher with Full Security.* SPACE 2021: 22–41, 2021.

B. Chakraborty, S. Chattopadhyay, A. Jha, M. Nandi: *On Length Independent Security Bounds for the PMAC Family.* IACR Trans. Symmetric Cryptol. 2021(2): 423–445, 2021.

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 comprehensive list is available on DBLP.