Ashwin Jha

Fakultät für Informatik MC 1.40
Symmetrische Kryptographie
Ruhr-Universität Bochum
Universitätsstr. 140
44801 Bochum, Germany

India
Germany
21 July, 1991
170/3669
migfi

ashwin.jha@outlook.de
https://ashwin-jha.github.io/
ashwin-jha-crypto
0000-0001-5957-2837
(+49) 1517 510 3739

Research Interests

I primarily work in cryptography, with a focus on the provable security of symmetric-key constructions in both classical and post-quantum settings. My research focuses on developing and applying statistical, algebraic, and combinatorial techniques to derive tight security bounds for symmetric-key modes of operation.

Education

Jun. 2020 | **PhD in Computer Science**
ISI Kolkata, India
Thesis: Provable Security of Symmetric-key Cryptographic Schemes
Advisor: Prof. Mridul Nandi

July 2015 | **Master of Technology in Computer Science**
ISI Kolkata, India
First Class with Distinction | Best Dissertation Gold Medal
Thesis: Cryptanalysis of Iterated Hash and Its Variants
Advisor: Prof. Mridul Nandi

June 2012 | **Bachelor of Engineering in Computer Engineering**
Delhi College of Engineering, University of Delhi, India
First Class

Research Experience

Jan. 2024 – present | **CaSa Jump.Start Post-doc**
HGI, RUB, Germany

Jan. 2021 – Dec. 2023 | **Post-doc**
CISPA, Germany

Jul. 2015 – Jun. 2020 | **Research Fellow**
ASU, ISI Kolkata, India

Research Visits and Internships

Jul. 2020 – Dec. 2020 | **Visiting Scientist**
R. C. Bose Centre, ISI Kolkata, India

Jan. 2018 – Mar. 2018 | **Research Intern**
Fujitsu Labs. of America, USA

Aug. 2017 – Oct. 2017 | **Research Intern**
NTT Secure Platform Labs. Tokyo, Japan

Mentoring Experience

Autumn 2024 | Universal Hashing in the Ideal Cipher Model
Sougata Mandal
PhD Research Internship | RUB, Germany

Spring 2024 | Constrained Systems
Abishanka Saha
PhD Research Internship | RUB, Germany

Spring 2022 | On Large Tweaks in Tweakable Even-Mansour
Soumya Kanti Saha
Masters' Research Internship | CISPA, Germany
(Part of the masters' thesis work submitted at ISI Kolkata, India)

Summer 2019 | Automated MILP Modeling for Cryptanalysis
Swastik Banerjee and Suvraneel Chatterjee
Summer Internship | ISI Kolkata, India

Teaching Experience

Fall 2025 | Symmetric Cryptanalysis
Faculty of Computer Science | RUB, Germany
Role: Co-instructor

Autumn 2020 | Advanced Cryptology
M. Tech. (C&S) | ISI Kolkata, India
Role: Co-instructor

Autumn 2018 | Cryptology
M. Tech. (CS) | ISI Kolkata, India
Role: Co-instructor

Autumn 2018 | Computing Systems I
M. Tech. (C&S) | ISI Kolkata, India
Role: Teaching assistant

Spring 2017 | Number Theory
B. Stat. | ISI Kolkata, India
Role: Teaching assistant

Autumn 2015 | Data and File Structures Lab.
M. Tech. (CS) | ISI Kolkata, India
Role: Teaching assistant

Selected Invited Talks

Aug. 2025 | **Evasive Properties: A Gap in the Quantum Oracles Zoo**
MAS Seminar | NTU, Singapore

Dec. 2024 | **Evasive Properties: A Gap in the Quantum Oracles Zoo**
ASK 2024 | TCG CREST Kolkata, India

Nov. 2022 | **Reset-Sampling: Fine-tuning the Security of Standardized MACs**
CRC Seminar Series | TII, Abu Dhabi

Jul. 2020 | **Towards an Improved Bound on CBC Collision Probability and Its Applications**
India Crypto Meet | Online

Invited Workshop Participations

Asian Workshop on Symmetric-Key Cryptography

Dec. 2024	Kolkata, India
Nov. 2018	Kolkata, India
Sep. 2016	Nagoya, Japan
Oct. 2015	Singapore

Lorentz Center Workshop

Apr. 2024	On Beating Real-Time Crypto: Solutions and Analysis Leiden, Netherlands
Mar. 2018	On Flexible Cryptography Leiden, Netherlands

Dagstuhl Seminar on Symmetric Cryptography

Jan. 2024	Schloss Dagstuhl, Germany
Apr. 2022	Schloss Dagstuhl, Germany

Sep. 2022	Frisiacrypt 2022 Terschelling, Netherlands

Refereeing and Community Services

Editorial/Program Committee Memberships

2026, 2025	ACM CCS (Applied Cryptography Track)
2025	IACR ASIACRYPT
2025 – 2026	IACR Transactions on Symmetric Cryptology
2022 – 2024	IACR Transactions on Symmetric Cryptology
2023, 2022	International Conference on Cryptology And Network Security (CANS)

Journal/External Refereeing Services

2025	Journal of Cryptology
2020 – 2025	Design, Codes and Cryptography
2023	IEEE Transactions on Information Theory
2021 – 2023	IET Information Security
2016 – 2025	IACR CRYPTO, EUROCRYPT, ASIACRYPT
2016	IACR FSE

Workshop Organization

Sep. 2025	First Workshop on Generic Attacks and Proofs in Symmetric Cryptography NTU, Singapore

Publications

2025

On the Number of Restricted Solutions to Constrained Systems and their Applications
ASIACRYPT 2025 | Cogliati, *Jha*, Naccache, Nandi, Saha

Post-quantum Security of Key-Alternating Feistel Ciphers
ASIACRYPT 2025 | Basak, Bhaumik, Chauhan, Jejurikar, *Jha*, Roy, Schrottenloher, Talnikar

Cryptographic Treatment of Key Control Security – In Light of NIST SP 800-108
CRYPTO 2025 | Bhaumik, Dutta, Inoue, Iwata, *Jha*, Minematsu, Nandi, Sasaki, Turan, Tessaro

On TRP-RF Switch in the Quantum Query Model
IACR Commun. Cryptol. | *Jha*

Generic Security of GCM-SST
ACNS 2025 | Inoue, *Jha*, Mennink, Minematsu

Towards Optimally Secure Deterministic Authenticated Encryption Schemes
EUROCRYPT 2025 | Chen, Dutta, *Jha*, Nandi

2024

Mind the Bad Norms: Revisiting Compressed Oracle-based Quantum Indistinguishability Proofs
ASIACRYPT 2024 | Bhaumik, Cogliati, Ethan, *Jha*

Tight Security of TNT and Beyond: Attacks, Proofs and Possibilities for the Cascaded LRW Paradigm
EUROCRYPT 2024 | *Jha*, Khairallah, Nandi, Saha

2023

On Large Tweaks in Tweakable Even-Mansour with Linear Tweak and Key Mixing
IACR ToSC 2023(4) | Cogliati, Ethan, *Jha*, Saha

Revisiting Randomness Extraction and Key Derivation Using the CBC and Cascade Modes
IACR ToSC 2023(4) | Balachandran, *Jha*, Nandi, Pal

On Quantum Secure Compressing Pseudorandom Functions
ASIACRYPT 2023 | Bhaumik, Cogliati, Ethan, *Jha*

Revisiting the Indifferentiability of the Sum of Permutations
CRYPTO 2023 | Gunsing, Bhaumik, *Jha*, Mennink, Shen

Subverting Telegram's End-to-End Encryption
IACR ToSC 2023(1) | Cogliati, Ethan, *Jha*

2022

Towards Tight Security Bounds for OMAC, XCBC and TMAC
ASIACRYPT 2022 | Chattopadhyay, *Jha*, Nandi

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

2021

Fine-Tuning the ISO/IEC Standard LightMAC
ASIACRYPT 2021 | Chattopadhyay, *Jha*, Nandi

Revisiting the Security of COMET Authenticated Encryption Scheme
INDOCRYPT 2021 | Gueron, *Jha*, Nandi

tHyENA: Making HyENA Even Smaller
INDOCRYPT 2021 | Chakraborti, Datta, *Jha*, Mancillas-López, Nandi

Elastic-Tweak: A Framework for Short Tweak Tweakable Block Cipher
INDOCRYPT 2021 | Chakraborti, Datta, *Jha*, Mancillas-López, Nandi, Sasaki

Light-OCB: Parallel Lightweight Authenticated Cipher with Full Security
SPACE 2021 | Chakraborti, Datta, *Jha*, Mancillas-López, Nandi

On Length Independent Security Bounds for the PMAC Family
IACR ToSC 2021(2) | Chakraborty, Chattopadhyay, *Jha*, Nandi

2020

How to Build Optimally Secure PRFs Using Block Ciphers
ASIACRYPT 2020 | Cogliati, *Jha*, Nandi

Tight Security of Cascaded LRW2
J. Cryptology 33(3) | *Jha*, Nandi

On the Security of Sponge-type Authenticated Encryption Modes
IACR ToSC 2020(2) | Chakraborty, *Jha*, Nandi

From Combined to Hybrid: Making Feedback-based AE even Smaller
IACR ToSC 2020(S1) | Chakraborti, Datta, *Jha*, Mitragotri, Nandi

ESTATE: A Lightweight and Low Energy Authenticated Encryption Mode
IACR ToSC 2020(S1) | Chakraborti, Datta, *Jha*, Mancillas-López, Nandi, Sasaki

2019

INT-RUP Secure Lightweight Parallel AE Modes
IACR ToSC 2019(4) | Chakraborti, Datta, *Jha*, Mancillas-López, Nandi, Sasaki

On Random Read Access in OCB
IEEE Trans. Information Theory 65(12) | *Jha*, Mancillas-López, Nandi, Sen Gupta

2018 | **On Rate-1 and Beyond-the-Birthday Bound Secure Online Ciphers using Tweakable Block Ciphers**
Cryptography and Communications 10(5) | *Jha*, Nandi

2017 | **XHX - A Framework for Optimally Secure Tweakable Block Ciphers from Classical Block Ciphers and Universal Hashing**
LATINCRYPT 2017 | *Jha*, List, Minematsu, Mishra, Nandi

A New Look at Counters: Don't Run Like Marathon in a Hundred Meter Race
IEEE Trans. Computers 66(11) | Dutta, *Jha*, Nandi

Tight Security Analysis of EHtM MAC
IACR ToSC 2017(3) | Dutta, *Jha*, Nandi

On The Exact Security of Message Authentication Using Pseudorandom Functions
IACR ToSC 2017(1) | *Jha*, Mandal, Nandi

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

Selected Preprints

A Game-theoretic Interpretation of Backdoors in Cryptosystems
Jha

Evasive Properties: A Gap in the Quantum Oracles Zoo
Jha

Indifferentiability of 6-round Feistel Network
Bhaumik, *Jha*, Nandi, Paul, Saha

Awards and Grants

2024 – 2025 | CaSa Jump.Start Post-doc Grant
DFG under EXC 2092 CaSa – 39078197 | RUB, Germany

2021 | Lightweight Crypto Challenge Prize
Data Security Council of India and MeitY, Government of India

2015 – 2020 | ISI Doctoral Research Fellowship
MoSPI, Government of India | ISI Kolkata, India

2015 | Suniti Kumar Gold Medal
Best Dissertation Award | ISI Kolkata, India

2014 | Google Summer of Code Fellowship
Google

References

Prof. Mridul Nandi
ISI Kolkata, India
mridul@isical.ac.in

Prof. Tetsu Iwata
Nagoya University, Japan
iwata.tetsu.f6@f.mail.nagoya-u.ac.jp

Prof. Bart Mennink
Maastricht University, Netherlands
bart.mennink@maastrichtuniversity.nl

Dr. Kazuhiko Minematsu
NEC Corporation Kawasaki, Japan
k-minematsu@nec.com

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

Dr. Yu Sasaki
NTT Secure Platform Labs. Tokyo, Japan
yusk.sasaki@ntt.com