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
JYqmpTYAAAAJ

ashwin.jha@outlook.de
https://ashwin-jha.github.io/
ashwin-jha-crypto
0000-0001-5957-2837
263858
(+49) 1517 510 3739

Research Interests

I work primarily in cryptography, focusing on practice-oriented provable security of symmetric-key cryptography – the backbone of modern cryptographic infrastructure – in both classical and post-quantum settings. This includes designing efficient constructions, developing novel security models to capture evolving real-world threats, and developing statistical and combinatorial tools that yield tight security guarantees for symmetric-key constructions under minimal assumptions, thereby improving both the security and the efficiency of real-world cybersecurity apparatus.

Beyond cryptography, I am interested in research problems at the intersection of cryptography and related fields, including cybersecurity, combinatorics, statistics, and complexity theory.

Education

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

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

Jun. 2012 | **Bachelor of Engineering in Computer Engineering**
Delhi College of Engineering, University of Delhi, India
First Class (*magna cum laude*)

Research Experience

Jan. 2024 – present | **Post-doc**
HGI, RUB, Germany | DFG-funded CASA Jump.Start Post-doc Grant
Provable security of symmetric-key cryptography against advanced adversaries.

Jan. 2021 – Dec. 2023 | **Post-doc**
CISPA, Germany
Provable security of symmetric-key cryptography in the real-world.

Jul. 2015 – Jun. 2020 | **Doctoral Research Fellow**
ASU, ISI Kolkata, India
Design and provable security analysis of symmetric-key constructions.

Research Visits and Internships

Jul. 2020 – Dec. 2020 | **Visiting Scientist**
R. C. Bose Centre, ISI Kolkata, India
Design and provable security analysis of lightweight AEAD constructions.

Jan. 2018 – Mar. 2018 | **Research Intern**
Fujitsu Labs. of America, USA
Quantum cryptanalysis of modes of operations.

Aug. 2017 – Oct. 2017 | **Research Intern**
NTT Secure Platform Labs. Tokyo, Japan
Provable security of tweakable block cipher-based PRFs and MACs.

Pedagogical Experience

Teaching Experience

Fall 2025 | **Symmetric Cryptanalysis**
M. Sc. (CS) | RUB, Germany
Co-instructor | Developed and delivered lectures on generic attack techniques.

Fall 2020 | **Advanced Cryptology**
M. Tech. (C&S) | ISI Kolkata, India
Co-instructor | Delivered lectures on mathematical foundations of cryptology.

Fall 2018 | **Cryptology**
M. Tech. (CS) | ISI Kolkata, India
Co-instructor | Delivered lectures on symmetric-key cryptology.

Fall 2018 | **Computing Systems I**
M. Tech. (C&S) | ISI Kolkata, India
Teaching assistant | Delivered tutorial sessions.

Spring 2017 | **Number Theory**
B. Stat. | ISI Kolkata, India
Teaching assistant | Delivered tutorial sessions and lectures on computational number theory.

Fall 2015 | **Data and File Structures Lab.**
M. Tech. (CS) | ISI Kolkata, India
Teaching assistant | Delivered tutorial sessions and lectures on advanced C programming.

Mentoring Experience

Fall 2024 | **Universal Hashing in the Ideal Cipher Model**
Sougata Mandal (TCG CREST, India)
PhD Research Internship | RUB, Germany

Spring 2024 | **Constrained Systems**
Abishanka Saha (ISI Kolkata, India)
PhD Research Internship | RUB, Germany
Led to a publication in IACR ASIACRYPT 2025.

Spring 2022 | **On Large Tweaks in Tweakable Even-Mansour**
Soumya Kanti Saha (ISI Kolkata, India)
Master's Thesis | CISPA, Germany
Led to a publication in IACR ToSC.

Summer 2019 | **Automated MILP Modeling for Cryptanalysis**
Swastik Banerjee (SRM Institute of Science & Technology, India)
Bachelor's Thesis | ISI Kolkata, India

Selected Invited Talks

Mar. 2026 | **Constrained Systems**
ASK 2026 | NTU, Singapore
Formulation of a combinatorial tool and its applications in provable security.

Aug. 2025 | **Evasive Properties: A Gap in the Quantum Oracles Zoo**
MAS Seminar | NTU, Singapore
Characterising a class of quantum lower bound problems hard for quantum oracle-based techniques.

Dec. 2024 | **Evasive Properties: A Gap in the Quantum Oracles Zoo**
ASK 2024 | TCG CREST Kolkata, India
Characterising a class of quantum lower bound problems hard for quantum oracle-based techniques.

Nov. 2022 | **Reset-Sampling: Fine-tuning the Security of Standardized MACs**
CRC Seminar Series | TII, Abu Dhabi
New proof technique and its application in the provable security analysis of MAC algorithms.

Jul. 2020 | **Towards an Improved Bound on CBC Collision Probability and Its Applications**
India Crypto Meet | Online
New results on the collision probability of CBC-MAC.

Invited Workshop Participations

Asian Workshop on Symmetric-Key Cryptography

Mar. 2026, Oct. 2015	Singapore
Dec. 2024	Kolkata, India
Nov. 2018	Kolkata, India
Sep. 2016	Nagoya, Japan

Lorentz Center Workshop

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

Dagstuhl Seminar on Symmetric Cryptography

Jan. 2024, Apr. 2022	Schloss Dagstuhl, Germany

Other Workshops

Nov. 2025	Gelrecrypt 2025 Nijmegen, The Netherlands
Sep. 2022	Frisiacrypt 2022 Terschelling, The Netherlands

Refereeing and Community Services

Editorial/Program Committee Memberships

2027	IACR EUROCRYPT (invited)
2026, 2025	ACM CCS (Applied Cryptography Track)
2026, 2025	IACR ASIACRYPT
2025 – 2027	IACR Transactions on Symmetric Cryptology (ToSC)
2022 – 2024	IACR Transactions on Symmetric Cryptology (ToSC)
2026	Workshop on Selected Areas in Cryptography (SAC)
2023, 2022	International Conference on Cryptology And Network Security (CANS)

Journal/External Refereeing Services

2024, 2025	Journal of Cryptology
2020 – 2026	Design, Codes and Cryptography
2023	IEEE Transactions on Information Theory
2021 – 2023	IET Information Security
2016 – 2025	IACR CRYPTO, EUROCRYPT, ASIACRYPT
2025	USENIX Security Symposium
2016	IACR FSE

Workshop Organisation

Feb. 2026 – present | Online GAPS Seminar
Virtual event
Co-initiated a recurring virtual seminar on provable security of symmetric-key cryptography.

Sep. 2025 | First Workshop on Generic Attacks and Proofs in Symmetric Cryptography
GAPS 2025 | NTU, Singapore
Co-initiated a workshop on provable security of symmetric-key cryptography.

Awards and Grants

2024 – 2025 | CaSa Jump.Start Post-doc Grant
DFG under EXC 2092 CaSa – 39078197 | RUB, Germany
A total amount of €280,000 over two years.

2021 | Lightweight Crypto Challenge Prize
MeitY, Government of India | Data Security Council of India
A cash prize of ₹150,000.

2015 – 2020 | ISI Doctoral Research Fellowship
MoSPI, Government of India | ISI Kolkata, India
A total amount of ₹1,350,000 over five years.

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

2014 | Google Summer of Code Fellowship
Google
A total amount of $5,500 over six months.

List of Publications

Peer-reviewed: 35 | Top-tier publications (A*/A and Q1/Q2): 26 | Citations: 600+ | h-index: 15

2026 | **How to Build a Short-Input Random Oracle from Public Random Permutations**
EUROCRYPT 2026 | Bhaumik, Datta, Dutta, *Jha*, Mandal, Mennink, Nandi, Shen
DOI: 10.1007/978-3-032-25333-0_14
Taxonomy and provable security analyses of permutation-based short-input hash functions.

2025 | **On the Number of Restricted Solutions to Constrained Systems and their Applications**
ASIACRYPT 2025 | Cogliati, *Jha*, Naccache, Nandi, Saha
DOI: 10.1007/978-981-95-5018-0_18
Combinatorial tool beneficial in the provable security analysis of sum of permutation-type constructions.

Post-quantum Security of Key-Alternating Feistel Ciphers
ASIACRYPT 2025 | Basak, Bhaumik, Chauhan, Jejurikar, *Jha*, Roy, Schrottenloher, Talnikar
DOI: 10.1007/978-981-95-5018-0_15
Provable security analysis of key-alternating Feistel ciphers in the post-quantum setting.

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
DOI: 10.1007/978-3-032-01901-1_12
A novel security model formalising the key control attack on NIST SP 800-108 key derivation functions.

On TRP-RF Switch in the Quantum Query Model
IACR Commun. Cryptol. | *Jha*
DOI: 10.62056/a3waksuc2
General statistical result on the security of tweakable block ciphers in the quantum setting.

Generic Security of GCM-SST
ACNS 2025 | Inoue, *Jha*, Mennink, Minematsu
DOI: 10.1007/978-3-031-95764-2_14
Provable security analysis of a short-tag variant of GCM which is in consideration for IETF standardisation.

Towards Optimally Secure Deterministic Authenticated Encryption Schemes
EUROCRYPT 2025 | Chen, Dutta, *Jha*, Nandi
DOI: 10.1007/978-3-031-91107-1_1
Novel block cipher-based deterministic AEAD modes with optimal security.

2024

Mind the Bad Norms: Revisiting Compressed Oracle-based Quantum Indistinguishability Proofs
ASIACRYPT 2024 | Bhaumik, Cogliati, Ethan, *Jha*
DOI: 10.1007/978-981-96-0947-5_8
Discovering a flaw in the quantum security proof of the well-known Luby-Rackoff construction.

Tight Security of TNT and Beyond: Attacks, Proofs and Possibilities for the Cascaded LRW Paradigm
EUROCRYPT 2024 | *Jha*, Khairallah, Nandi, Saha
DOI: 10.1007/978-3-031-58716-0_9
Birthday-bound attack on TNT that invalidated its security claim.

2023

On Large Tweaks in Tweakable Even-Mansour with Linear Tweak and Key Mixing
IACR ToSC 2023(4) | Cogliati, Ethan, *Jha*, Saha
DOI: 10.46586/tosc.v2023.i4.330-364
Provable security analysis of the TWEAKEY tweakable block cipher design paradigm.

Revisiting Randomness Extraction and Key Derivation Using the CBC and Cascade Modes
IACR ToSC 2023(4) | Balachandran, *Jha*, Nandi, Pal
DOI: 10.46586/tosc.v2023.i4.391-419
Filling critical gaps in the proofs of a seminal result on the use of CBC as a randomness extractor.

On Quantum Secure Compressing Pseudorandom Functions
ASIACRYPT 2023 | Bhaumik, Cogliati, Ethan, *Jha*
DOI: 10.1007/978-981-99-8727-6_2
New framework for quantum indistinguishability proofs and its applications.

Revisiting the Indifferentiability of the Sum of Permutations
CRYPTO 2023 | Gunsing, Bhaumik, *Jha*, Mennink, Shen
DOI: 10.1007/978-3-031-38548-3_21
Attacks on the Sum of Permutations construction invalidating state-of-the-art indifferentiability bound.

Subverting Telegram's End-to-End Encryption
IACR ToSC 2023(1) | Cogliati, Ethan, *Jha*
DOI: 10.46586/tosc.v2023.i1.5-40
Efficient algorithm substitution attacks on MTProto2.0, the AEAD construction used in Telegram clients.

2022

Towards Tight Security Bounds for OMAC, XCBC and TMAC
ASIACRYPT 2022 | Chattopadhyay, *Jha*, Nandi
DOI: 10.1007/978-3-031-22963-3_12
Tight provable security analysis of OMAC, a NIST and ISO standardised MAC algorithm.

A Survey on Applications of H-Technique: Revisiting Security Analysis of PRP and PRF
Entropy 24(4) | *Jha*, Nandi
DOI: 10.3390/e24040462
Comprehensive survey on H-coefficients technique, a widely-used indistinguishability proof technique.

2021

Fine-Tuning the ISO/IEC Standard LightMAC
ASIACRYPT 2021 | Chattopadhyay, *Jha*, Nandi
DOI: 10.1007/978-3-030-92078-4_17
Novel proof techniques to reduce the key size of LightMAC, an ISO standardised MAC algorithm.

Revisiting the Security of COMET Authenticated Encryption Scheme
INDOCRYPT 2021 | Gueron, *Jha*, Nandi
DOI: 10.1007/978-3-030-92518-5_1
Design and analysis of COMET, a penultimate round candidate in NIST Lightweight Project.

tHyENA: Making HyENA Even Smaller
INDOCRYPT 2021 | Chakraborti, Datta, *Jha*, Mancillas-López, Nandi
DOI: 10.1007/978-3-030-92518-5_2
Design and analysis of tHyENA, winner of the Lightweight Crypto Challenge organised by DSCI.

Elastic-Tweak: A Framework for Short Tweak Tweakable Block Cipher
INDOCRYPT 2021 | Chakraborti, Datta, *Jha*, Mancillas-López, Nandi, Sasaki
DOI: 10.1007/978-3-030-92518-5_6
Generalised framework to turn a secure block cipher into a short-tweak tweakable block cipher.

Light-OCB: Parallel Lightweight Authenticated Cipher with Full Security
SPACE 2021 | Chakraborti, Datta, *Jha*, Mancillas-López, Nandi
DOI: 10.1007/978-3-030-95085-9_2
Highly efficient and lightweight variant of OCB AEAD.

On Length Independent Security Bounds for the PMAC Family
IACR ToSC 2021(2) | Chakraborty, Chattopadhyay, *Jha*, Nandi
DOI: 10.46586/tosc.v2021.i2.423-445
Characterisation of necessary properties to obtain length-independent bounds for PMAC-type MACs.

2020

How to Build Optimally Secure PRFs Using Block Ciphers
ASIACRYPT 2020 | Cogliati, *Jha*, Nandi
DOI: 10.1007/978-3-030-64837-4_25
General paradigm to construct optimally secure PRFs from block ciphers.

Tight Security of Cascaded LRW2
J. Cryptology 33(3) | *Jha*, Nandi
DOI: 10.1007/s00145-020-09347-y
Novel combinatorial and probabilistic tools to prove tight security bounds for cascaded LRW2.

On the Security of Sponge-type Authenticated Encryption Modes
IACR ToSC 2020(2) | Chakraborty, *Jha*, Nandi
DOI: 10.13154/tosc.v2020.i2.93-119
Functional graph-based analysis of Transform-then-Permute, a generalisation of Sponge-based AEAD schemes.

From Combined to Hybrid: Making Feedback-based AE even Smaller
IACR ToSC 2020(S1) | Chakraborti, Datta, *Jha*, Mitragotri, Nandi
DOI: 10.13154/tosc.v2020.iS1.417-445
Design and analysis of HyENA, a penultimate round candidate in NIST Lightweight Project.

ESTATE: A Lightweight and Low Energy Authenticated Encryption Mode
IACR ToSC 2020(S1) | Chakraborti, Datta, *Jha*, Mancillas-López, Nandi, Sasaki
DOI: 10.13154/tosc.v2020.iS1.350-389
Design and analysis of ESTATE, a penultimate round candidate in NIST Lightweight Project.

2019 **On Random Read Access in OCB**
IEEE Trans. Information Theory 65(12) | *Jha*, Mancillas-López, Nandi, Sen Gupta
DOI: 10.1109/TIT.2019.2925613
Optimised variant of OCB3 with random read access property.

INT-RUP Secure Lightweight Parallel AE Modes
IACR ToSC 2019(4) | Chakraborti, Datta, *Jha*, Mancillas-López, Nandi, Sasaki
DOI: 10.13154/tosc.v2019.i4.81-118
Design and analysis of LOTUS/LOCUS, penultimate round candidates in NIST Lightweight Project.

2018 **On Rate-1 and Beyond-the-Birthday Bound Secure Online Ciphers using Tweakable Block Ciphers**
Cryptography and Communications 10(5) | *Jha*, Nandi
DOI: 10.1007/s12095-017-0275-0
General paradigm to construct efficient and optimally secure online ciphers from tweakable block ciphers.

2017 **A New Look at Counters: Don't Run Like Marathon in a Hundred Meter Race**
IEEE Trans. Computers 66(11) | Dutta, *Jha*, Nandi
DOI: 10.1109/TC.2017.2710125
General framework for efficient and provably secure usage of counters in symmetric-key cryptography.

Tight Security Analysis of EHtM MAC
IACR ToSC 2017(3) | Dutta, *Jha*, Nandi
DOI: 10.13154/tosc.v2017.i3.130-150
Tight provable security analysis of randomised MAC, EHtM.

XHX - A Framework for Optimally Secure Tweakable Block Ciphers from Classical Block Ciphers and Universal Hashing
LATINCRYPT 2017 | *Jha*, List, Minematsu, Mishra, Nandi
DOI: 10.1007/978-3-030-25283-0_12
General framework to construct tweakable block ciphers using block ciphers and universal hashing.

On The Exact Security of Message Authentication Using Pseudorandom Functions
IACR ToSC 2017(1) | *Jha*, Mandal, Nandi
DOI: 10.13154/tosc.v2017.i1.427-448
Comprehensive and tight provable security analysis of CBC-based PRFs.

2016 **Revisiting Structure Graphs: Applications to CBC-MAC and EMAC**
J. Mathematical Cryptology 10(3–4) | *Jha*, Nandi
DOI: 10.1515/jmc-2016-0030
Discovering and fixing flaws in seminal results on the provable security of CBC-MAC and EMAC.

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, The Netherlands
bart.mennink@maastrichtuniversity.nl

Dr. Benoît Cogliati
Thales DIS France SAS, France
benoit-michel.cogliati@thalesgroup.com

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

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