Ritam Bhaumik

Date of Birth:	21 Jul. 1988
Address (Office):	Technology Innovation Institute, P. O. Box: 9639, Yas Island, Abu Dhabi, UAE
Phone:	+971 50 639 6255
Email (Work):	ritam.bhaumik@tii.ae
Email (Personal):	bhaumik.ritam@gmail.com
Website:	ritam-b.github.io
DBLP:	167/3093
OrcID:	0000-0002-2883-4870

Research Interests

At present I work primarily on classical and post-quantum security proofs for symmetric-key cryptosystems. My research focus is two-fold: (1) on identifying and studying provable security problems that can have a meaningful impact on real-life cryptographic protocols; (2) on finding ways in which classical proof techniques can be generically applied in post-quantum contexts. Other topics of interest for me include quantum and classical cryptanalysis of symmetric-key modes, indifferentiability of symmetric-key constructions against classical and quantum adversaries, and machine-learning-based distinguishing attacks on symmetric-key cryptosystems.

My doctoral research mostly focussed on the construction of modes of operation based on ideal small-domain primitives like random permutations and random functions, and coming up with reduction-proofs of their security guarantees using counting techniques and other tools of discrete probability. In the past I have looked at the possible application of cryptographic designs and protocols for enhancing privacy and security in blockchains and other decentralised networks. I have also looked at the applications of results from communication complexity in analysing space-time trade-offs in the cryptanalysis of modes.

Research Positions Held

Apr. 2024 – present	CRC, TII Abu Dhabi, UAE Position: Senior Researcher
Oct. 2022 – Mar. 2024	LASEC, EPFL, Switzerland Position: Post-doc
Mar. 2020 – Sep. 2022	COSMIQ, Inria Paris, France Position: Post-doc
Aug. 2013 – Dec. 2019	Cryptology Research Group, ASU, ISI Kolkata, India Position: Research Fellow Supervisor: Mridul Nandi
Aug. 2018 – Mar. 2019	SnT, University of Luxembourg, Luxembourg Position: Research Associate

Scientific Education

Dec. 2019	PhD in Computer Science ISI Kolkata Thesis title: Design and Provable Security of Symmetric-Key Modes Advisor: Mridul Nandi
May 2011	M. Stat. ISI Kolkata Specialisation: Mathematical Statistics and Probability
May 2009	B. Stat. (Hons.) ISI Kolkata

Publications

Post-quantum Security of Key-Alternating Feistel Ciphers. ASIACRYPT '25.[†]
Jyotirmoy Basak, *Ritam B.*, Amit Kumar Chauhan, Ravindra Jejurikar, Ashwin Jha, Anandarup Roy, André Schrottenloher, Suprita Talnikar.

Cryptographic Treatment of Key Control Security In Light of NIST SP 800-108. CRYPTO '25.
Ritam B., Avijit Dutta, Akiko Inoue, Tetsu Iwata, Ashwin Jha, Kazuhiko Minematsu, Mridul Nandi, Yu Sasaki, Meltem Sonmez Turan, Stefano Tessaro.

Building a BBB Pseudorandom Permutation using Lai-Massey Networks. Communications in Cryptology. 1(4).
Ritam B., Mohammad Amin Raeisi.

Block Cipher Doubling for a Post-Quantum World. Communications in Cryptology. 1(3).
Ritam B., André Chailloux, Paul Frixons, Bart Mennink, María Naya-Plasencia.

Mind the Bad Norms: Revisiting Compressed Oracle-based Quantum Indistinguishability Proofs. ASIACRYPT '24.
Ritam B., Benoît Cogliati, Jordan Ethan, Ashwin Jha.

Efficient Variants of TNT with BBB Security. ProvSec '24.
Ritam B., Bishwajit Chakraborty, Wonseok Choi, Avijit Dutta, Cuauhtemoc Mancillas López, Hrithik Nandi, Yaobin Shen.

Indifferentiability of Confusion-Diffusion Networks. SCN '24.
Ritam B., Mridul Nandi, Sayantan Paul, Abishanka Saha.

Provably Secure Online Authenticated Encryption and Bidirectional Online Channels. SAC '24.
Arghya Bhattacharjee, *Ritam B.*, Daniel Collins, Mridul Nandi.

The Committing Security of MACs with Applications to Generic Composition. CRYPTO '24.
Ritam B., Bishwajit Chakraborty, Wonseok Choi, Avijit Dutta, Jérôme Govinden, Yaobin Shen.

On Quantum-Secure Compressing Pseudorandom Functions. ASIACRYPT '23.
Ritam B., Benoît Cogliati, Jordan Ethan, Ashwin Jha.

BBB Security for 5-Round Even-Mansour-Based Key-Alternating Feistel Ciphers. Designs, Codes and Cryptography. 92(1).
Arghya Bhattacharjee, *Ritam B.*, Avijit Dutta, Mridul Nandi, Anik Raychaudhuri.

PAE: Towards More Efficient and BBB-secure AE From a Single Public Permutation. ICICS '23.
Arghya Bhattacharjee, *Ritam B.*, Avijit Dutta, Eik List.

[†]To appear (as of June '25).

Revisiting the Indifferentiability of the Sum of Permutations. CRYPTO '23.
Aldo Gunsing, *Ritam B.*, Ashwin Jha, Bart Mennink, Yaobin Shen.

Offset-Based BBB-Secure Tweakable Block-ciphers with Updatable Caches. INDOCRYPT '22.
Arghya Bhattacharjee, *Ritam B.*, Mridul Nandi.

A Sponge-Based PRF with Good Multi-user Security. SAC '22.
Arghya Bhattacharjee, *Ritam B.*, Mridul Nandi.

QCB: Efficient Quantum-secure Authenticated Encryption. ASIACRYPT '21.
Ritam B., Xavier Bonnetain, André Chailloux, Gaëtan Leurent, María Naya-Plasencia, André Schrottenloher, Yannick Seurin.

Improved Indifferentiability Security Proof for 3-Round Tweakable Luby-Rackoff. Designs, Codes and Cryptography. 89(10).
Ritam B., Mridul Nandi, Anik Raychaudhuri.

ZCZ: Achieving n-bit SPRP Security with a Minimal Number of Tweakable-Block-Cipher Calls. ASIACRYPT '18.
Ritam B., Eik List, Mridul Nandi.

Improved Security for OCB3. ASIACRYPT '17.
Ritam B., Mridul Nandi.

The Iterated Random Function Problem. ASIACRYPT '17.
Ritam B., Nilanjan Datta, Avijit Dutta, Nicky Mouha, Mridul Nandi.

Turning Online Ciphers Off. Transactions on Symmetric Cryptology. 2017(2).
Guy Barwell, *Ritam B.*, Daniel Page, Mridul Nandi, Martijn Stam.

OleF: An Inverse-Free Online Cipher. Transactions on Symmetric Cryptology. 2016(2).
Ritam B., Mridul Nandi.

An Inverse-Free Single-Keyed Tweakable Enciphering Scheme. ASIACRYPT '15.
Ritam B., Mridul Nandi.

Other Manuscripts

A Note on Feedback-PRF Mode of KDF from NIST SP 800-108.
Ritam B., Avijit Dutta, Tetsu Iwata, Ashwin Jha, Kazuhiko Minematsu, Mridul Nandi, Yu Sasaki, Meltem Sonmez Turan, Stefano Tessaro.

Permutation-based Parallelizable Short-Input Random Oracles.
Ritam B., Nilanjan Datta, Avijit Dutta, Ashwin Jha, Sougata Mandal, Bart Mennink, Hrithik Nandi, Yaobin Shen.

Pencil: A Domain-Extended BBB PRF for Strengthening GCM and More.
Ritam B., Jean Paul Degabriele, Chandranan Dhar.

Tweakable Involution Ciphers and Applications.
Ritam B., Bishwajit Chakraborty, Wonseok Choi, Avijit Dutta, Jérôme Govinden, Yaobin Shen.

BBB Secure Large-Tweak TBC from Ideal Block Ciphers.
Arghya Bhattacharjee, *Ritam B.*, Nilanjan Datta, Avijit Dutta, Shibam Ghosh, Sougata Mandal.

Universal Context Commitment without Ciphertext Expansion.
Arghya Bhattacharjee, *Ritam B.*, Chandranan Dhar, Ashwin Jha, Sougata Mandal.

Compromising Electromagnetic Emanations of Smartphone Touch Sensors.
Ritam B., Marin Huzar, Nathan Peluso, Jean-François Rocher, David Schmid, Antoine Sidem.

Indifferentiability of 6-round Feistel.
Ritam B., Ashwin Jha, Mridul Nandi, Sayantan Paul, Abishanka Saha.

Invited Research Workshop Participations

Feb. 2026	Dagstuhl Seminar on Symmetric Cryptography, Schloss Dagstuhl, Germany[1]
Sep. 2025	Generic Attacks and Proofs in Symmetric Cryptography, Singapore[1]
Dec. 2024	Asian Workshop on Symmetric-Key Cryptography, Kolkata, India
Jan. 2024	Dagstuhl Seminar on Symmetric Cryptography, Schloss Dagstuhl, Germany
Dec. 2023	Asian Workshop on Symmetric-Key Cryptography, Guangzhou, China
Sep. 2022	Frisiacrypt 2022, Terschilling, Netherlands
Apr. 2022	Dagstuhl Seminar on Symmetric Cryptography, Schloss Dagstuhl, Germany
Mar. 2018	Lorentz Workshop on Flexible Symmetric Cryptography, Leiden, Netherlands
Dec. 2017	Asian Workshop on Symmetric-Key Cryptography, Changsha, China
Sep. 2016	Asian Workshop on Symmetric-Key Cryptography, Nagoya, Japan
Oct. 2015	Asian Workshop on Symmetric-Key Cryptography, Singapore

Refereeing Service

Editor for Transactions on Symmetric Cryptology (2024—present), Communications in Cryptology (2025—present).

Reviewer for Designs, Codes and Cryptography (2021—2024).

Sub-reviewer for ASIACRYPT '25, ACM CCS '25, CRYPTO '25, EUROCRYPT '25, CT-RSA '25, EUROCRYPT '24, ACNS '24, ASIACRYPT '23, CRYPTO '23, EUROCRYPT '23, FSE '22, CRYPTO '22, EUROCRYPT '21, FSE '21, CRYPTO '21, CRYPTO '20, EUROCRYPT '19, CT-RSA '19, Financial Cryptography '19, FSE '16, EUROCRYPT '16.

Supervision

Tapping Electromagnetic Emanations from a Smartphone Touchscreen. 2023, EPFL.
Marin Thomas Michel Huzar (masters' project, Autumn 2023).
Nathan Peluso (masters' project, Autumn 2023).
Antoine Sidem (masters' thesis, Spring 2023).[4]
David Schmid (masters' project, Spring 2023).
Jean-François Rocher (bachelors' project, Spring 2023).

Attacking Pseudorandomness with Deep Learning. 2023, EPFL.
Benjamin Krieger (masters' project, Autumn 2023).
Ana-Maria Indreias (masters' project, Autumn 2023).
Wei-En Hsieh (bachelors' project, Autumn 2023).
Jean-Baptiste Michel (masters' project, Spring 2023).

Quantum Cryptanalysis of Symmetric-Key Modes. 2023, EPFL.
Valentina Iliescu (masters' project, Autumn 2023).
Lancelot Scheid (masters' project, Spring 2023).

Tight Security Bounds for Lai-Massey Schemes. 2023, EPFL.
Mohammad Amin Raeisi (internship, Summer 2023).

A Deeper Look at Compressed Permutation Oracles. 2023, EPFL.
Gehad Salem (internship, Summer 2023).

A Survey on Advanced Techniques in Symmetric Cryptanalysis. 2023, EPFL.
Nilabha Saha (internship, Summer 2023).

Mirror Theory through Simulations. 2023, EPFL.
Luca Maier (masters' project, Spring 2023).

[1] Upcoming (as of June '25).
[4] Awarded the Kudelski Prize 2023 for the best masters' thesis in security.

Shorter Stays and Research Visits

Feb. 2023	LIP6, Sorbonne Université Paris, France
Dec. 2022	Cryptology Research Group, ASU, ISI Kolkata, India
May 2022	LASEC, EPFL, Switzerland
Nov. 2021 – Jan. 2022	Cryptology Research Group, ASU, ISI Kolkata, India
Mar. 2018	LASEC, EPFL, Switzerland
Apr. – May 2016	COSIC, KU Leuven, Belgium

Project Participations

2022 – 2023	BioID (PI: Serge Vaudenay, EPFL)
2020 – 2022	QUASYModo (PI: María Naya-Plasencia, Inria Paris)
2018 – 2019	FinCrypt (PI: Alex Biryukov, University of Luxembourg)

Teaching Experience

Spring 2023	Substitute Teacher, **Advanced Cryptography** (COM-501), EPFL
Autumn 2019	Substitute Teacher, **Probability Theory** (M. Math.), ISI Kolkata
Spring 2016	Substitute Teacher, **Graph Theory** (M. Math.), ISI Kolkata

References

Mridul Nandi.
Professor at ISI Kolkata, India.
Email: mridul.nandi@gmail.com.

Jean Paul Degabriele.
Principal Researcher at Technology Innovation Institute, Abu Dhabi, UAE.
Email: jeanpaul.degabriele@tii.ae.

Serge Vaudenay.
Professor at EPFL, Switzerland.
Email: serge.vaudenay@epfl.ch.

María Naya-Plasencia.
Directeur de Recherche at Inria Paris, France.
Email: maria.naya_plasencia@inria.fr.

Bart Mennink.
Associate Professor at Radboud University Nijmegen, Netherlands.
Email: b.mennink@cs.ru.nl.