Ritam Bhaumik

Date of Birth:	21 Jul. 1988
Address (Home):	Ch. de Rionza 15, 1020 Renens, Switzerland
Address (Office):	INF 238, EPFL, 1015 Lausanne, Switzerland
Phone:	+41 76 516 20 49
Email (Work):	ritam.bhaumik@epfl.ch
Email (Personal):	bhaumik.ritam@gmail.com
Website:	ritam-b.github.io

Research Interests

At present I work primarily on post-quantum security proofs for symmetric-key cryptosystems. My research focus is 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, applications of provably secure symmetric-key schemes in messaging protocols and other practical scenarios, 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.

Positions Held

Oct. 2022 – present	LASEC, EPFL, Switzerland Position: Post-doc Supervisor: Serge Vaudenay
Mar. 2020 – Sep. 2022	COSMIQ, Inria Paris, France Position: Post-doc (till Feb. 2021) | SRP (since Mar. 2021) Supervisor: María Naya-Plasencia
Aug. 2013 – Dec. 2019	Cryptology Research Group, ASU, ISI Kolkata Position: JRF (till Aug. 2015) | SRF (since Aug. 2015) Supervisor: Mridul Nandi

Scientific Education

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

Publications

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. Design, 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.

Preprints under Review

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

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

Robust Online Authenticated Encryption and Bidirectional Online Channels.
Arghya Bhattacharjee, *Ritam B.*, Daniel Collins, Mridul Nandi.

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

Block-cipher Doubling for a Post-Quantum World.
Ritam B., André Chailloux, Paul Frixons, Bart Mennink, María Naya-Plasencia.

BBB Security for 5-Round Even-Mansour-Based Key-Alternating Feistel Ciphers.
Arghya Bhattacharjee, *Ritam B.*, Avijit Dutta, Mridul Nandi, Anik Raychaudhuri.

Invited Research Workshop Participations

Sep. 2022	Frisiacrypt 2022, Terschilling, Netherlands
Apr. 2022	Dagstuhl Seminar on Symmetric Cryptography, Schloss Dagstuhl, Germany
Mar. 2018	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

Shorter Stays and Research Visits

Feb. 2023	LIP6, Sorbonne Université Paris, France
Dec. 2022	Cryptology Research Group, ASU, ISI Kolkata
May 2022	LASEC, EPFL, Switzerland
Nov. 2021 – Jan. 2022	Cryptology Research Group, ASU, ISI Kolkata
Aug. 2018 – Mar. 2019	SnT, University of Luxembourg, Luxembourg
Mar. 2018	LASEC, EPFL, Switzerland
Apr. – May 2016	COSIC, KU Leuven, Belgium

Project Participations

2022 – present	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

Refereeing Service

Reviewer for Design, Codes and Cryptography.

Sub-reviewer for ASIACRYPT '23, CRYPTO '23, EUROCRYPT '23, FSE '22, CRYPTO '22, EUROCRYPT '21, FSE '21, CRYPTO '21, CRYPTO '20, EUROCRYPT '19, CT-RSA '19, FC '19, FSE '16, EUROCRYPT '16.

Supervision

Tapping Electromagnetic Emanations from a Smartphone Touchscreen. Spring 2023, EPFL.
Antoine Sidem (masters' thesis), David Schmid (masters' project), Jean-François Rocher (bachelors' project).

Attacking Pseudorandomness with Deep Learning. Spring 2023, EPFL.
Jean-Baptiste Michel (masters' project).

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

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

References

Mridul Nandi[1], Serge Vaudenay[2], María Naya-Plasencia[3], Bart Mennink[4].

[1]Professor at ISI Kolkata, India. Email: mridul.nandi@gmail.com
[2]Professor at EPFL, Switzerland. Email: serge.vaudenay@epfl.ch
[3]Directeur de Recherche at Inria Paris, France. Email: maria.naya_plasencia@inria.fr
[4]Associate Professor at Radboud University, Nijmegen, Netherlands. Email: b.mennink@cs.ru.nl