Ritam **Bhaumik**

RESEARCHER IN A STARTING RESEARCH POSITION (SRP), CRYPTOGRAPHY

65 Avenue Louis Aragon, 94800 Villejuif, France

(+33) 6-56-86-20-49 | ✉ bhaumik.ritam@gmail.com

"The generation of random numbers is too important to be left to chance."
Robert R. Coveyou

Research Experience

POSITIONS HELD

Institut national de recherche en informatique et en automatique — *Paris, FR*

STARTING RESEARCH POSITION (SRP) — *March 2021 - Present*

- PROJECT: QUASYModo
- PROJECT LEADER: María Naya-Plasencia
- TEAM: COSMIQ
- RESEARCH AREA: Symmetric Post-Quantum Cryptography

Institut national de recherche en informatique et en automatique — *Paris, FR*

POSTDOCTORAL RESEARCHER — *March 2020 - Feb 2021*

- PROJECT: QUASYModo
- PROJECT LEADER: María Naya-Plasencia
- TEAM: COSMIQ
- RESEARCH AREA: Symmetric Post-Quantum Cryptography

Indian Statistical Institute — *Kolkata, IN*

RESEARCH FELLOW IN COMPUTER SCIENCE — *August 2013 - December 2019*

- THESIS ADVISOR: Mridul Nandi
- DEPARTMENT: Applied Statistics Unit, Applied Statistics Division
- TEAM: Cryptology Research Group
- PRIMARY AREA OF RESEARCH: Provable Security in the Symmetric-Key setting

University of Luxembourg — *Esch-sur-Alzette, LU*

RESEARCH ASSOCIATE — *August 2018 - March 2019*

- PROJECT: FinCrypt
- PROJECT LEADER: Alex Biryukov
- DEPARTMENT: The Interdisciplinary Centre for Security, Reliability and Trust
- TEAM: CryptoLUX
- RESEARCH AREA: Privacy in Blockchains

EPFL — *Lausanne, CH*

VISITING SCHOLAR (SHORT VISIT) — *March 2018*

- SPONSOR: Serge Vaudenay
- TEAM: LASEC

KU Leuven — *Leuven, BE*

VISITING SCHOLAR — *April 2016 - May 2016*

- SPONSOR: Bart Preneel
- TEAM: COSIC
- COLLABORATOR: Bart Mennink
- RESEARCH AREA: Provably Secure Constructions

SUMMARY OF INTERESTS

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 my last research position I looked at the possible application of cryptographic designs and protocols for enchancing 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 tradeoffs in the cryptanalysis of modes. Currently I am working on post-quantum security proofs for symmetric-key encryption systems. My research focus is finding ways in which classical proof techniques can be generically applied in post-quantum contexts.

Topics I've Worked on

Mode Design: Symmetric-Key

- Length-Preserving Wide Permutations
- Tweakable Wide Permutations
- Compressing Functions
- Online Permutations
- Modes on Public Primitives
- Domain Extension of Blockciphers

Security Goals: Symmetric-Key

- Indistinguishability against CPA/CCA
- Integrity against Forging Attacks
- Security Beyond the Birthday-Bound
- Multi-User Security
- Indifferentiability
- Security against Quantum Adversaries

Proof Techniques: Symmetric-Key

- Coefficient H Technique
- Lazy Sampling of Quantum Primitives
- Post-Quantum Proofs Based on Databases

Blockchains

- Proofs of Sequential Work
- Controlled Resource-Hardness
- Space-Time Tradeoffs in Proofs of Space
- Accumulators from Bilinear Groups
- Zero-Knowledge Proofs

Topics I Plan to Explore in the Future

- Consensus Protocols
- Security Amplifications
- Card-Based Protocols
- Automating Proofs of Correctness
- Lightweight Cryptography
- Generic Proof Frameworks (Classical/Post-Quantum)
- Quantum Cryptanalysis

Publications

QCB: Efficient Quantum-secure Authenticated Encryption

ASIACRYPT 2021, Proceedings (to appear) *Springer 2021*

- Co-Authors: Xavier Bonnetain, André Chailloux, Gaëtan Leurent, María Naya-Plasencia, André Schrottenloher and Yannick Seurin
- Editors: Mehdi Tibouchi and Huaxiong Wang
- Link to Preprint: https://eprint.iacr.org/2020/1304

Improved Indifferentiability Security Proof for 3-Round Tweakable Luby-Rackoff

Design, Codes and Cryptography, Volume 89, Number 10 *Springer 2021*

- Co-Authors: Mridul Nandi and Anik Raychaudhuri
- Pages: 2255-2281
- Link: https://link.springer.com/article/10.1007%2Fs10623-021-00913-4

ZCZ - Achieving n-bit SPRP Security with a Minimal Number of Tweakable-Block-Cipher Calls

LNCS 11272

ASIACRYPT 2018, Proceedings, Part I — *Springer 2018*

- Co-Authors: Eik List and Mridul Nandi
- Editors: Thomas Peyrin and Steven D. Galbraith
- Pages: 336–366
- Link to Preprint: https://eprint.iacr.org/2018/819

Improved Security for OCB3

LNCS 10625

ASIACRYPT 2017, Proceedings, Part II — *Springer 2017*

- Co-Author: Mridul Nandi
- Editors: Tsuyoshi Takagi and Thomas Peyrin
- Pages: 638–666
- Link to Preprint: https://eprint.iacr.org/2017/845

The Iterated Random Function Problem

LNCS 10625

ASIACRYPT 2017, Proceedings, Part II — *Springer 2017*

- Co-Authors: Nilanjan Datta, Avijit Dutta, Nicky Mouha and Mridul Nandi
- Editors: Tsuyoshi Takagi and Thomas Peyrin
- Pages: 667–697
- Link to Preprint: https://eprint.iacr.org/2017/892

Turning Online Ciphers Off

Transactions on Symmetric Cryptology, Volume 2017, Issue 2 — *2017*

- Co-Authors: Elene Andreeva, Guy Barwell, Daniel Page, Mridul Nandi and Martijn Stam
- Editors: Florian Mendel and María Naya-Plasencia
- Pages: 105–142
- Link: https://tosc.iacr.org/index.php/ToSC/article/view/640/608

OleF: An Inverse-Free Online Cipher

Transactions on Symmetric Cryptology, Volume 2016, Issue 2 — *2016*

- Co-Author: Mridul Nandi
- Editors: María Naya-Plasencia and Bart Preneel
- Pages: 30–51
- Link: https://tosc.iacr.org/index.php/ToSC/article/view/564/506

An Inverse-Free Single-Keyed Tweakable Enciphering Scheme

LNCS 9453

ASIACRYPT 2015, Proceedings, Part II — *Springer 2015*

- Co-Author: Mridul Nandi
- Editors: Tetsu Iwata and Jung Hee Cheon
- Pages: 159–180
- Link to Preprint: https://eprint.iacr.org/2015/1148

Education

Indian Statistical Institute

Kolkata, IN

Ph.D. — *August 2013 - December 2019*

- Thesis Title: Design and Provable Security Analysis of Symmetric-Key Modes
- Thesis Advisor: Mridul Nandi

Indian Statistical Institute

Kolkata, IN

M.Stat. — *July 2009 - May 2011*

- Specialisation: Mathematical Statistics and Probability
- Aggregate Score: 61.5%
- Select Courses: Advanced Probability, Advanced Stochastic Process, Advanced Design of Experiments, Optimisation Techniques

Indian Statistical Institute

Kolkata, IN

B.Stat. (Hons.) — *July 2006 - May 2009*

- Aggregate Score: 70%
- Select Courses: Probability Theory, Statistical Methods, C and Data Structures, Linear Models, Algebra, Analysis, DBMS

Refereeing Experience

Journal Reviewer

- Design, Codes and Cryptography

Subreviewer

- CRYPTO (2021, 2020)
- EUROCRYPT (2021, 2019, 2016)
- ToSC (2021-1, 2021-3, 2021-4)
- CT-RSA (2019)
- Financtial Cryptography (2019)
- FSE (2016)

Teaching Experience

Teaching Assistant

Probability Theory *Kolkata, IN*

M.Math. 2nd Year, Indian Statistical Institute *Fall 2019*

Graph Theory *Kolkata, IN*

M.Math. 2nd Year, Indian Statistical Institute *Spring 2016*

Skills and Strengths

Mathematics

- Combinatorics
- Discrete Probability
- Linear Algebra
- Logic (Propositional, First-Order, Modal)
- Elementary Number Theory

Computer Science

- Design of Algorithms
- Graph Theory
- Imperative Programming (C, C++, Python)
- Functional Programming (Haskell, ML, Racket)

Miscellaneous Strengths

- Analytical Approach to Problem Solving
- Abstract Thinking
- Quick Learner
- Native Fluency in English
- Elementary Knowledge of German and French

Other Areas of Interest

Stuff I Follow Other People Doing

- Experimental and Arthouse Cinema
- Literature
- Philosophy
- Linguistics
- Classical, Folk and Country Music
- Tennis
- Football

STUFF I TRY DOING MYSELF

- Writing
- Learning the Classical Guitar
- Filmmaking
- Learning Languages
- Coding
- Photography

References

Mridul Nandi *Kolkata, IN*
INDIAN STATISTICAL INSTITUTE `mridul.nandi@gmail.com`

María Naya-Plasencia *Paris, FR*
INRIA `maria.naya_plasencia@inria.fr`

Bart Mennink *Nijmegen, NL*
RADBOUD UNIVERSITY `b.mennink@cs.ru.nl`

Nicky Mouha *Gaithersburg, MD, US*
NIST `nicky@mouha.be`