

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 | 🏠 ritam-b.github.io



"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 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 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

PUBLICATIONS

QCB: Efficient Quantum-secure Authenticated Encryption

LNCS 13090

ASIACRYPT 2021, PROCEEDINGS, PART I

Springer 2021

- CO-AUTHORS: Xavier Bonnetain, André Chailloux, Gaëtan Leurent, María Naya-Plasencia, André Schrottenloher and Yannick Seurin
- EDITORS: Mehdi Tibouchi and Huaxiong Wang
- PAGES: 668–698
- 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

SUB-REVIEWER

- CRYPTO (2021, 2020)
- EUROCRYPT (2021, 2019, 2016)
- ToSC (2021-1, 2021-3, 2021-4)
- CT-RSA (2019)
- Financial 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
- Programming (C, C++, Python, Haskell, ML, Racket)

MISCELLANEOUS STRENGTHS

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

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