Ritobroto Maitra

Junior Year, Computer Science

Snail Mail

Room A-723,
Boys' Hostel - 1,
IIT Patna,
Bihar - 801118
India

Tel & Skype

+91 7044 165 665
+44 745 2231 444
ritobroto.maitra94

Mail

ritobrotomaitra@
gmail.com
ritobroto.ee13@
iitp.ac.in

Web & Git

ritobrotom.com
Git - jethroFloyd

Programming

Working Knowledge
C
F*
F#, F7
Python
OCaml
PHP/SQL
Bash
HTML/CSS
Familiar
TeX
Coq
JavaScript
Haskell
ML
Scala / ScalaCheck
Magma / Maple
Matlab
Java
Basic Knowledge
C++
Django

OS Familiarity

OS X ★★★★★
Kali Linux ★★★★
Windows ★★★★
Ubuntu ★★★

Research Projects

05/14 - Now **Cryptanalysis of SHA-Family Hash Functions** IIIT Delhi, India

Automated Cryptanalysis of SHA-1 and SHA-2. We are working on developing tools that automatically search for hash collisions.

Position: Research Intern

Mentor: **Dr. Somitra Sanadhya**, IIIT Delhi, India and University of Haifa, Israel

06/15 - 04/17 **Language-Based Information Flow Security Analysis** IIT Patna, India

We are working on developing frameworks for language-based information flow security analysis, using formal methods and abstract interpretation of programming languages. We are building toolkits for this as well, starting with PHP and moving to other languages. This is also part of my work for my B.Tech thesis.

Position: Research Student

Mentor: **Dr. Raju Halder**, IIT Patna

12/14 - 01/16 **Reverse Engineering:Constant Weight Encoding Functions** CNRS, France

Reverse engineering and generalization of the constant weight encoding functions in HyMES. Developing software for automated techniques.

Position: Visiting Research Student

Mentor: **Dr. Pierre-Louis Cayrel**, Hubert Curien Laboratory, University of Saint-Etienne

05/15 - 09/15 **Algebraic Cryptanalysis** Loughborough University, UK

Modelling stream ciphers like ZUC, Trivium and Snow as algebraic systems, deriving their controlling equations using Möbius Transforms, and then using derivatives of the Cube attack for automated attacks. Generalizing the Cube Attack for higher order differentials.

Position: Visiting Research Student

Mentor: **Prof. Ana Salagean**, Loughborough University

05/15 - 08/15 **Post-Quantum and Quantum Security Proofs** GuardTime

Rigorous post-quantum security proofs for GuardTime's proprietary algorithms in a real-time scenario. Migration of existing security proofs from a classical to a quantum setting.

Position: Research Intern.

Mentor: **Hema Krishnamurthy**, Vice President, Research, GuardTime

06/14 - 06/15 **Analysis of Crime HotSpots** IIT Patna, India

Crime Analysis using Pattern Recognition. Using machine learning algorithms such as AMOSA and NSGA-II on real data sets of criminal activities in a geospatial setting and using it to predict areas and times of increased criminal activity - like a crime hotspot.

Position: Research Intern

Mentor: **Dr. Sriparna Saha**, IIT Patna

10/14 - Now **theAttendanceProject : Incubated Start-Up** Seed funding: WhizMantra

Development of a secure embedded device for scalable fingerprint authentication under low-power restrictions and consequent data processing.

Position: Head, Technical Operations

01/15 - Now **jethroFloyd - Start-Up** Funding: Indian Angel Network

Head of Technical Operations, development and maintenance of online platform. Development of a virtual trial room for fashion shopping online.

Position: CEO

Languages

English - Fluent (Verbal and Written)
Bengali - Mother Tongue (Verbal and Written)
Hindi - Near-native (Verbal and Written)
French - Learning!

Interests

Music and Poetry
Neorealist Cinema
Capture the Flag
Thinking
Hacking
Minesweeper
Football
Ethics and the Net
Ethics and AI
Privacy and the Society
Photography
Entrepreneurship
Adda
Open-source
Wildlife

Education

2013 - 2017 **Bachelor of Technology - Computer Science and Engineering**
Indian Institute of Technology, Patna
Junior Year (5th Semester) - CPI - 8.91 (on a scale of 10)
Student Coordinator, Computer Science and Electronics Incubation
Student Coordinator, Computer Science Research Groups

1999 - 2013 **Higher Secondary Education** South Point High School, Kolkata
Graduated with a Percentile of 99.99 and Ranked 14th in the State.
Main subjects: Mathematics, Physics, Chemistry, Statistics and Languages

Research Interests

Cryptology and Security
Symmetric Key cryptanalysis, Post-quantum security, Coding-theory based systems, Anonymity and Privacy

Programming Languages and Formal Methods
Formal Methods, Security Analysis, Program Verification, Automated Testing and Proof Assistants, Information Flow Security

Machine Learning
Pattern Recognition, Learning, Genetic Algorithms

Workshops and Conferences

12/2014 **ASK 2014** SETS, Chennai, India
Worked under Dr. Nicky Mouha on Automated Cryptanalysis.
Society for Electronic Transactions and Security, Chennai

01/2015 **Real World Crypto 2015** London School of Economics, London, UK
Local Organizer: Dr. Kenny Paterson, Royal Holloway

12/2014 **INDOCRYPT 2014** India Habitat Centre, Delhi, India
Scientific Analysis Group, DRDO, under the aegis of CRSI

12/2014 **Interplay of Statistics and Cryptology - Workshop, 2014** ISI, Kolkata, India
Applied Statistics Unit, Indian Statistical Institute

Extra-curricular Responsibilities

07/14 - 05/16 **Coordinator, Start-Up Relations Cell**
Entrepreneurship Club, IIT Patna
Building an incubation centre for start-ups and building a panel of mentors and investors, encouraging and building an entrepreneurial mindset in the campus through various events, internships and jobs at start-ups, launching and maintaining a webzine with a focus on this area.

07/14 - 02/15 **Sub-coordinator, Cultural Committee**
Anwesha 2015, Annual Techno-Cultural Fest, IIT Patna
Managing the cultural division of a festival with an outreach of more than 20,000 people.