Ritobroto Maitra

CSE | Sophomore

Snail Mail

Room 212,
Ashoka Hall,
IIT Patna,
Patna - 800013
Bihar, India

Tel & Skype

+91 7762 99 0626
ritobroto.maitra94

Mail

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

Web & Git

ritobrotom.com
Git - jethroFloyd
LinkedIn

Programming

C	★★★★★
Java	★★★★★
HTML	★★★★★
PHP, SQL	★★★★
Python	★★★★
Shell	★★★★
Matlab	★★★
Scala	★★★
C++	★★★
JavaScript	★★★
Magma	★★
Maple	★★
Assembly	★★
Wolfram	★★
FORTRAN	★★
Haskell	★
R	★
C #	★
Lisp	★

OS Preference

Ubuntu	★★★★★
Fedora	★★★★
Windows	★★★★
Kali	★★★
MacOS	★★★

Experience

05/14 - Now **Cryptanalysis of SHA-Family Hashes** IIIT Delhi, India
Study, design and implementation of attacks against the SHA-Family hash functions, with a special emphasis on SHA-2.
Position: Research Intern
Mentor: **Dr. Somitra Kr Sanadhya**, IIIT Delhi

06/14 - Now **Analysis of Crime HotSpots** IIT Patna, India
Analysis of Crime Hotspots using Clustering and Pattern Recognizing Algorithms like AMOSA.
Position: Research Intern
Research Partner - Don K. Dennis, IIT Patna
Mentor: **Dr. Sriparna Saha**, IIT Patna

10/14 - Now **McBits Cryptanalysis** Centre National de la Recherche Scientifique, France
Study and cryptanalysis of the McBits Cryptosystem. Exploiting the scheme for attacks on hash functions. Side Channel Attacks.
Position: Off-Campus Intern, Campus Visit Scheduled for Winter 2015.
Mentor: **Dr. Pierre-Louis Cayrel**, CNRS

05/14 - 05/16 **Post-Quantum Code-Based Cryptosystems** Research and Analysis Wing, India
Investigation, implementation and improvement of coding theory based cryptosystems like the McEliece Cryptosystem.
Position: Research Associate
Funding: **Defence Research and Development Organization**, India

10/14 - 12/14 **theAttendanceProject** WhizMantra
Design of a scalable prototype that records students' attendance with minimal chance of human tampering and works in areas without electricity and mobile network coverage.
Position: Project Leader

Education

2013 - 2017 **Bachelor of Technology - Computer Science and Engineering**
Indian Institute of Technology, Patna
Currently in 3rd Semester with CPI - 9.4 (on a scale of 10)
Main Coursework: (I - Independent)
Number Theory, Linear Algebra, Cryptology (I), Probability, Data Structures, Algorithms, Hardware-Software Interface (I), Coding Theory (I), Computational Complexity Theory (I), Discrete Maths

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, Computer Science

Languages

English	★★★★★
Bengali	★★★★★
Hindi	★★★★
French	★★★
German	★★

Research Interests

Cryptology
Cryptology and Network Security, Hash Functions, Protocols, Multi-Party Computations, Ciphers, Key Management, Provable Security, Authentication, Cloud Security and Public-Key Encryption.

Machine Learning
Pattern Recognition, Genetic Algorithms

Workshops and Conferences

12/2014 **ASK 2014** SETS, Chennai, India
Selected for participation in the Fourth Asian Workshop on Symmetric Cryptography.
Society for Electronic Transactions and Security, Chennai

12/2014 **INDOCRYPT 2014** India Habitat Centre, Delhi, India
Will participate in INDOCRYPT 2014 as an undergraduate student under the mentorship of Dr. Somitra Sanadhya.
Scientific Analysis Group, DRDO, under the aegis of CRSI

12/2014 **Interplay of Statistics and Cryptology - Workshop, 2014** ISI, Kolkata, India
Selected for participation in the Winter School on Interplay of Statistics and Cryptology.
Applied Statistics Unit, Indian Statistical Institute

Positions of Responsibility

07/14 - Now **Task Manager, Start-Up Relations Cell**
Entrepreneurship Club, IIT Patna

07/14 - Now **Sub-coordinator, Cultural Committee**
Anwesha 2015, Annual Techno-Cultural Fest, IIT Patna

References

IIIT Delhi **Dr. Somitra Kr. Sanadhya**
Ph.D., ISI, Kolkata
Asst. Professor, Dept. of CSE, IIIT Delhi, India
somitra@iiitd.ac.in
Site:https://sites.google.com/a/iiitd.ac.in/somitra/

IIT Patna **Dr. Sriparna Saha**
Ph.D., ISI, Kolkata
Asst. Professor, Dept. of CSE, IIT Patna, India
sriparna@iitp.ac.in
Site: http://www.iitp.ac.in/ sriparna/

Updated November, 2014

Ritobroto Maitra