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 ★★★★★
OCaml ★★★★
Python ★★★★
Shell ★★★★
Django ★★★
Matlab ★★★
Ruby/Rails ★★★
PHP/SQL ★★★
JavaScript ★★★
Assembly ★★★
Scala ★★
C++ ★★
Magma ★★
Sage ★★
Maple ★★
FORTRAN ★★
Haskell ★
R ★
C # ★
Lisp ★

OS Familiarity
Ubuntu ★★★★★
Windows ★★★★
Kali ★★★
MacOS ★★★

Ritobroto Maitra
Computer Science | Crypto | Entrepreneur

Experience
05/14 - Now **Cryptanalysis of SHA-Family Hashes** IIIT Delhi, India
Automated Cryptanalysis Techniques on SHA-1 and SHA-2.
Position: Research Intern
Mentor: **Dr. Somitra Kr Sanadhya**, IIIT Delhi

06/14 - Now **Analysis of Crime HotSpots** IIT Patna, India
Crime Analysis using Pattern Recognition and AI.
Position: Research Intern
Mentor: **Dr. Sriparna Saha**, IIT Patna

10/14 - Now **McBits Cryptanalysis** Centre National de la Recherche Scientifique, France
Efficient implementation and exploits on McBits Scheme.
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 of McEliece-type Cryptosystems.
Position: Research Associate
Funding: **Defence Research and Development Organization**, India

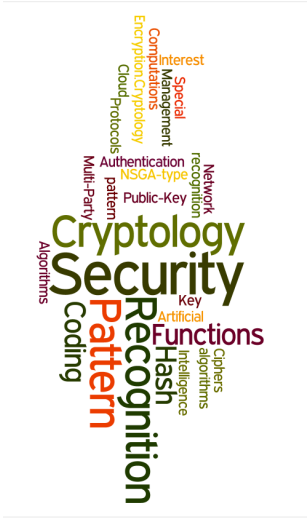
10/14 - 12/14 **theAttendanceProject : Incubated Start-Up** Seed funding: WhizMantra
Development of Secure Embedded Device for authentication under severe light-weight restrictions and consequent data processing.
Position: Chief

01/15 - 04/15 **H-RAM** IIT Patna, India
Complete Hostel Management including Room Allocation and Selection, Ticket Resolutions and Geo-tagged Lost-and-Found Services and in-built IM.
Position: Project Member

01/15 - 02/15 **4-Bit CPU** IIT Patna, India
Design and Implementation of a 4-Bit CPU.
Position: Project Member

Education
2013 - 2017 **Bachelor of Technology - Computer Science and Engineering**
Indian Institute of Technology, Patna
Currently in 4th Semester with CPI - 9.1 (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, Software and Systems Engineering, Digital Design, Hardware Programming, VHDL

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



Languages

English ★★★★★
Bengali ★★★★★
Hindi ★★★★
French ★★★
German ★★
Italian ★★
Urdu ★★

Research Interests

Cryptology
Cryptology and Network Security, Privacy and Security, Public Policy and Open-Source Solutions in Security, Hash Functions, Protocols, Multi-Party Computations, Ciphers, Key Management, Provable Security, Authentication, Cloud Security and Public-Key Encryption.

Machine Learning
Pattern Recognition, Neural Networks, 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

Positions of Responsibility

07/14 - Now **Task Manager, Start-Up Relations Cell**
Entrepreneurship Club, IIT Patna
Coordinating internships and placements at start-ups, building a start-up ecosystem in campus and mentoring campus start-ups.

07/14 - Now **Sub-coordinator, Cultural Committee**
Anwesha 2015, Annual Techno-Cultural Fest, IIT Patna
Coordinating cultural competitions and professional shows by internationally acclaimed outfits in a fest with an outreach and attendance of more than 20,000 people.

References

IIIT Delhi **Dr. Somitra Kr. Sanadhya**
Ph.D., ISI, Kolkata
Asst. Professor, Dept. of CSE, IIIT Delhi, India
Currently Visiting Prof. Orr Dunkelman, Haifa, Israel.
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/