ARKA RAI CHOUDHURI

PERSONAL INFORMATION
Email: arkarai.choudhuri@gmail.com
Email: cs1428@isical.ac.in
Ph No: +917044239266
Webpage: http://www.isical.ac.in/∼cs1428/

ADDRESS
Room 20, Meghnad Saha Hall,
Indian Statistical Institute,
205 B.T. Road, Kolkata,
India - 700108

RESEARCH INTEREST

My primary research interest is in **cryptography**. I am also interested in some other aspects of theoretical computer science.

EDUCATION

Master of Technology in Computer Science 2014-present
Indian Statistical Institute, Kolkata
Aggregate Marks: 93 %
Rank 1/28

Bachelor of Technology in Computer Science 2010-2014
National Institute of Technology Karnataka, Surathkal
CGPA: 8.53

Class 12 CBSE Computer Science, Mathematics, Physics and Chemistry 2010
Kendriya Vidyalaya IISc, Bangalore
Aggregate Marks: 94.2%

Class 10 CBSE 2008
Kendriya Vidyalaya IISc, Bangalore
Aggregate Marks: 92.8%

RESEARCH EXPERIENCE

Differential Cryptanalysis of Salsa and ChaCha - An Evaluation with a Hybrid Model
Advisor: Prof. Subhamoy Maitra Masters Thesis, August 2015 - Ongoing
Applied Statistics Unit,
Indian Statistical Institute

Recently there has been a discussion to make ChaCha20 a standard, and this in turn emphasizes the need for scrutiny and cryptanalysis of the same. In an attempt to provide greater conjectured security, unnecessarily high number of rounds are prescribed for the ciphers, sacrificing performance. Taking into account the existing differential attacks on reduced versions of Salsa and ChaCha, we propose a hybrid model, a simple tool to evaluate the security of ARX based constructions. We show, under certain assumptions, only 12 rounds of Salsa and ChaCha can be considered sufficient instead of the 20 proposed in these standards. The work is currently under submission and updates will appear **on my website.**

Privacy Applications with Imperfect Randomness
Advisor: Dr. Divesh Aggarwal June 2015 - Ongoing
Supervisor: Prof. Serge Vaudenay
Security and Cryptography Laboratory (LASEC),
École polytechnique fédérale de Lausanne (EPFL)

A common abstraction in Cryptography is to assume that there is a source of truly random bits available to all the participants in the system (cryptographic primitive). This is a highly unrealistic assumption and in practice, cryptographic systems have to be based on imperfect

sources of randomness. The question of whether privacy requires true randomness is hence a relevant question. In an important result by Bosley and Dodis, it was shown, for encryption, that unless the key size is exponential in that of the message, there is a need for extraction. But the proof cannot be extended to other primitives. We are attempting to prove that a secure 2-out-2 secret sharing scheme, a generalization of encryption, would imply extraction from the source. The work is ongoing, and we have made considerable progress towards a final result. Updates will appear **on my website.**

Budget Optimization in Sponsored Search Markets
Advisor: Prof. Swapan Bhattacharya — Undergraduate Thesis, July 2013 - May 2014
Department of Computer Science and Engineering,
NITK Surathkal

We looked, from the advertisers point of view, at the process of budget optimization. The advertiser, with their limited budget would like to spend, in the bidding process, on keywords that would maximize their profit. We looked at the different models of the problem, and concentrated our work on a variant of the multi armed bandit problem. Specifically, we focused on the performance of the Annealing Softmax on a specific model of the problem.
Due the lack of computational resources, we were not able to test out hypothesis on large datasets, and picked smaller datasets we thought were representative of large data.
The report can be found here - **MajorProject.pdf**

The MD5 Hash Function: A detailed study
Advisor: Prof. C.E. Veni Madhavan — May 2013 - July 2014
Department of Computer Science and Automation,
Indian Institute of Science

As a part of the Indian Academy of Sciences summer research fellowship programme, this project was to study the cryptographic primitive of hash functions. In particular, we looked at MD5. While MD5 at the time was already broken, the goal was to perform a detailed study of the various techniques used, barring the use of tunnelling. Our work also involved implementation of some of the simpler attacks and look for possible improvements.
A brief report of the study can be found here - **IASReport.pdf**

Dynamic Pricing Scheme in Social Networks
Advisor: Prof. P. Santhi Thilagam — Jan 2014 - May 2014
Department of Computer Science and Engineering,
NITK Surathkal

This was a part of a social networking project with Prof. Santhi Thilagam. We looked at various ideas for Dynamic Pricing in social networks, which is a relevant topic to many of the major online retailers. Our targets were two-fold, optimizing profit and keeping buyers satisfied. We came up with a dynamic strategy that takes advantage of the goods that a buyer purchases and also the amount of influence they exert in the social network. We look at both myopic and non-myopic models to design and compare strategies.
The work is under submission, and update will be available **on my website.**

An Incentivized Approach for Fair Participation in Wireless Ad hoc Networks
Advisor: Prof. Annappa B — Jan 2013 - May 2013
Department of Computer Science and Engineering,
NITK Surathkal

It started out as a course project, and then moved to be a research project. We looked at the problem of selfish nodes in ad hoc networks. These nodes just use the network for their own interest and refuse to relay data from other nodes in order to increase their own lifetime. This in turn brings down the productivity of the whole network. We developed an incentivized approach for participation in ad hoc networks. Given the routing path, we determine the power saving

contributed by each intermediate hop. We then use the cooperative game theoretic concept of Shapley Value to calculate the worth of each node. This is converted in virtual currency, which can then be later used by the nodes for data transmission.
The preprint version of the paper can be found at - **http://arxiv.org/pdf/1503.01314v1**

PUBLICATIONS

- Arka Rai Choudhuri, Subhamoy Maitra, "Differential Cryptanalyis of Salsa and ChaCha - An Evaluation with a Hybrid Model". In submission.
- Choudhuri, Arka Rai; S, Kalyanasundaram; Sridhar, Shriyak; B, Annappa. "An Incentivized Approach for Fair Participation in Wireless Ad hoc Networks". *International Journal of Recent Development in Engineering and Technology 2, no. 3 (2014): 117-121*
- Chetan Dugar; Arka Rai Choudhuri; Sriniketh Vijayaraghavan; Santhi Thilagam . "Dynamic Pricing Scheme in Social Networks". In submission.

PROFESSIONAL ACTIVITIES

External reviewer for: EUROCRYPT'16

SELECTED COURSEWORK

Masters: Cryptology, Abstract Algebra, Probability and Stochastic Processes, Optimization Techniques, Quantum Information Processing and Quantum Computing, Discrete Mathematics, Automata, Design and Analysis of Algorithms.
Undergraduate: Number Theory and Cryptography, Information Security, Linear Algebra, Advanced Data Structures and Algorithms.

SCHOLASTIC ACHIEVEMENTS

- Rank 1 (out of 28) in M.Tech Computer Science at Indian Statistical Institute Kolkata.
- Selected for the Summer@EPFL research internship programme for the summer of 2015.
- Placed 10^{th} in the country in the National Cyber Olympiad for the year 2010.
- Selected as Summer Research Fellow by the Indian Academy of Sciences for the summer of 2013.
- Reached the national round of the National Talent Search Examination of 2008. Awarded the state scholarship for the same.

SCHOOLS AND CONFERENCES

- Winter School on *Interplay Between Statistics and Cryptology* December 2014, at Indian Statistical Institute.
- Workshop on *Number Theory and Cryptology* held at National Institute of Technology Karnataka, Surathkal in 2013.
- *IC Research Day 2015* held at EPFL during the summer of 2015.
- *Yahoo! Summer School for Information Retrieval and the Semantic Web* held at Indian Institute of Science during the summer of 2013.
- Participant at the *Turing Centenary Conference* held at PESIT Bangalore during the summer of 2012.

SKILL SET

Technical Skills Quite proficient in coding in C and Python. Have additionally worked on bash, VHDL, x86 assembly language, Sage and GMP. Worked extensively on both Linux and Windows. Comfortable using LaTeX.
Languages: Fluent in English and Bengali. Have a good working knowledge of Hindi and Kannada.

EXTRACURRICULAR ACTIVITIES

- Was the captain of the University football team at National Institute of Technology for the academic year 2013-14.
- Trained in Hindustani classical Tabla for 7 years.
- Member of the Literary, Stage and Debating society at NITK as a part of the quiz team.
- Head of the computer special interest group of the Institution of Engineers, NITK chapter.
- Head boy of the school for the academic year 2009-10.

REFERENCES

Prof. Subhamoy Maitra
Thesis advisor
Professor at the Applied Statistics Unit, Indian Statistical Institute.
Webpage: **http://www.isical.ac.in/∼subho/**
Contact: subho@isical.ac.in

Prof. Serge Vaudenay
Research internship mentor
Professor at at the Swiss Federal Institute of Technologies (EPFL).
Webpage: **http://lasec.epfl.ch/∼vaudenay/**
Contact: serge.vaudenay@epfl.ch

Dr. Goutam Paul
Course advisor
Assistant Professor at the R. C. Bose Centre for Cryptology and Security, Indian Statistical Institute.
Webpage: **http://www.isical.ac.in/∼goutam.paul/**
Contact: goutam.paul@isical.ac.in