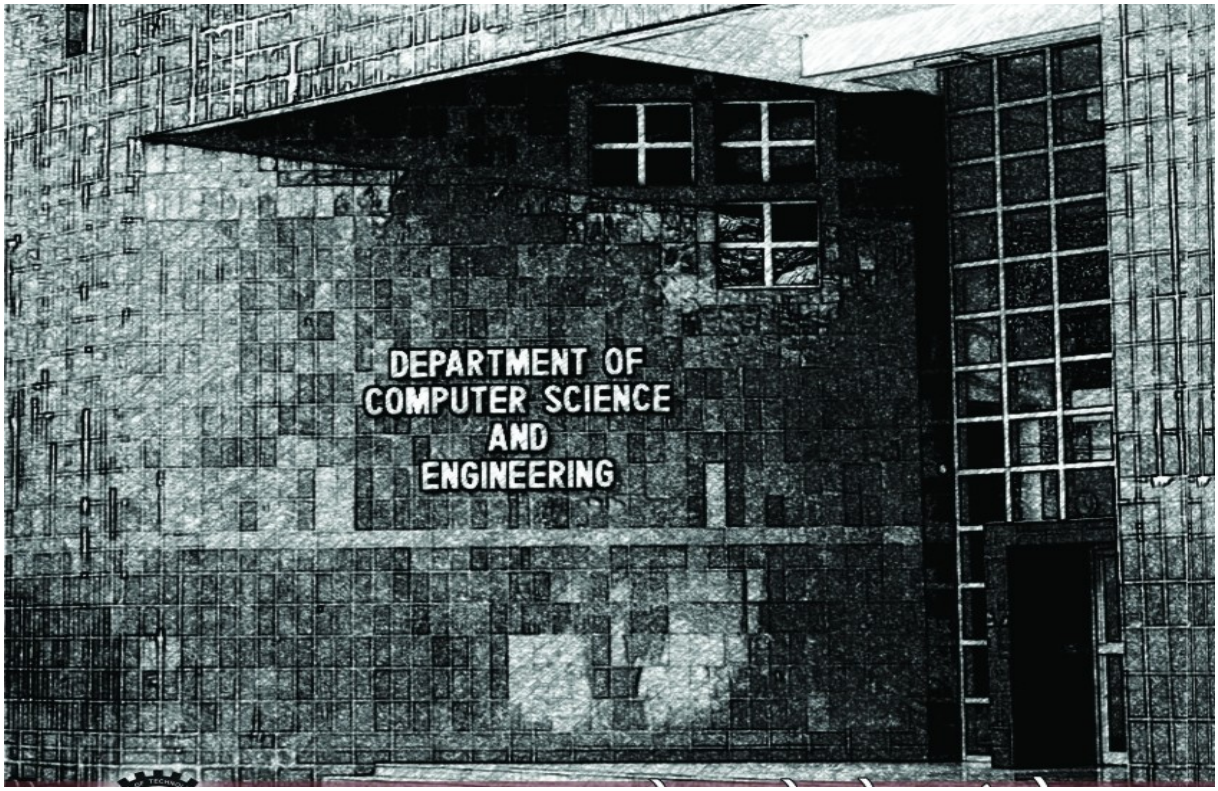


The Department of Computer Science & Engineering was initiated in 1980 and the first B.Tech. batch graduated in 1982. Apart from being the department producing the first batch of graduates in Computer Science and Engineering amongst the Indian Institutes of Technology, this is one of the most reputed centers for Computer Science education and research in the country.

The hallmarks of the department are in the breadth of its academic curricula and diversity in fundamental research and industrial collaborations. Collaborative research is ongoing with researchers in internationally acclaimed universities and research institutions abroad and in India such as USC, TIFR Mumbai, ISI Kolkata, RRI Bangalore, Perimeter Institute of Theoretical Physics, and SAC Bangalore. The Department has long-term research partnerships with leading companies such as Intel, National Semiconductors, Microsoft, General Motors, Synopsys, Sun Microsystems and Texas Instruments.

The alumni of this department are well established all over the globe achieving excellence in professional fields as well as in academics and research, and holding positions of rare distinction in leading industries and academic institutions of the world.

The sixth Research Scholar Day is going to be celebrated on the 15th day of March, 2015. This event gives the research students and the faculty members a unique opportunity to share and exchange research ideas and to build a complete picture of the research activity carried out by the research scholars in the department. The day also provides the research scholars with a platform to publicly demonstrate their cultural aptitude. Like the previous years, this year too the day will be observed with enthusiasm and zeal by our PhD and MS students. Let me wish this event a grand success!

Rajib Mall
Head of the Department

The photo of the CSE on Page 1 was taken from the cover page of the Research Scholar Day 2014 brochure which was designed by Romil Roy. The pictures, used on the back cover, were taken from the departmental photo albums. The cover-design team includes M. Srinivas Virinchi and Dhiman Saha. The production team for this brochure consists of Sabyasachi Karati, Subhrangsu Mandal and Shiladitya Ghosh. Other volunteers include Ashok Das, Bappa Chowdhury, Rajesh, Somyadip Bandyopadhyay, and Sourya Bhattacharyya. Help and cooperation from all research scholars, faculty members, and staff members of the CSE Department are highly appreciated.

List of Current PhD Scholars

Abantika Pal
Abhijnan Chakraborty
Abhik Jana
Abir De
Anju P J
Anupam Mandal
Aritra Hazra
Aritra Mahapatra
Ayan Das
Barnali Das
Bijju Kranthi Veduruparthi
Bruto Da Costa Antonio Anastasio
Debapriya Basu Roy
Debashis Mukherjee
Dhiman Saha
Durga Prasad Sahoo
Gaurav Saxena
Jimmy Jose
Joy Chandra Mukherjee
Kamalesh Ghosh
Koustav Rudra
Kunal Banerjee
Manjira Sinha
Mayank Singh
Moumita Saha
Mousumi Roy
Pankaj Kumar
Papia Mahato
Parantapa Bhattacharya
Partha Sarathi Dey
Pritam Bhattacharya
Priyanka Sinha
Rajendra Prasath R
Rajib Lochan Jana
Rajorshee Raha
Ranita Biswas
Sandipan Sikdar
Sanjoy Pratihar
Sarani Bhattacharya
Saranya Saha
Saurav Kumar Ghosh
Sayan Mandal
Shyantani Maiti
Soumadip Biswas
Soumajit Pramanik
Soumyadip Bandyopadhyay
Sounak Sadhukhan
Sourav Kumar Dandapat
Sourya Bhattacharyya
Sreejith M
Subhrangsu Mandal
Sudakshina Datta
Sudipta Saha
Suhansanu Kumar
Suman Kalyan Maity
Sumana Ghosh
Sumanta Pyne
Swapan Maiti
Tanmoy Chakraborty
Tanwi Mallick
Tapas Kumar Mishra
Tirthankar Dasgupta
Tripti Swarnkar
Urbi Chatterjee

List of Current MS Scholars

Abhishek Chakraborty
Anirban Ghose
Ayan Banerjee
K Sai Ram
Poulami Das
Sankarshan Mridha
Shamit Ghosh
Sonam Singh
Abhrajit Sengupta
Ankan Mullick
Debasmita Lohar
Paheli Bhattacharya
Prabir Mallick
Sayandeep Saha
Shiladitya Ghosh
Sulagna Gope

PhD Scholars

Abantika Pal
Email: abantika0pal@gmail.com
Joined CSE department in: December 2014

Abantika Pal *received a B.Tech. Degree in Computer Science Engineering from Academy of Technology under West Bengal University of Technology in 2011, and a M.E. Degree in Computer Science & Engineering from Jadavpur University in 2014. She has worked in Tata Consultancy Services, Kolkata from March,2012 to July,2012. Since December, 2014, she has been a reserch scholar in the department of Computer Science and Engineering of IIT Kharagpur. Her research interests are in the areas of Bioinformatics and Computational Biology.*

Supervisor: Prof. Pralay Mitra

Protein Interactor Discovery

One of the most widely used experimental techniques to determine the protein structures at the atomic level resolution is crystallography. Unfortunately, protein complex crystallization is more like an art than science. Identifying the protocols for the crystallization of protein molecule is one of the most challenging jobs in molecular biology. The process gets complicated by the fact that not all protein complexes are crystallizable. Although the problem is of great importance in molecular biology, but very less amount of work has done on this.

To address this, we are trying to develop a method that will check whether a protein complex will crystallize or not. If not then who else should partner with the existing protein molecule so that it will be crystallizable. We are testing the co-crystallizability of a protein complex using the knowledge of the protein-protein/ligand docking algorithms. For unsuitable cases, our plan is to design the complementary partner that will initiate and stabilize crystallization process.

Abhik Jana
Email: abhik.jana@cse.iitkgp.ernet.in
Joined CSE department in: January 2015

Abhik Jana *received a B.Tech. degree in Computer Science & Engineering from Institute of Engineering and Management in 2011 and an M.Tech. degree in Computer Science & Engineering from Indian Institute of Technology Kharagpur in 2013. From July 2013 till July 2014, he worked in a research group in NetApp India Pvt. Ltd . From August 2014 till December 2014 he was working as Senior Research Fellow in Computer Science & Engineering department in Indian Institute of Technology, Kharagpur. Since Jan 2015 he has been a research scholar in the department of Computer Science & Engineering in IIT Kharagpur. His research interests are in the areas of Natural Language Processing, Cognitive computing.*

Supervisor: Prof. Pawan Goyal

Abhijnan Chakraborty
Email: chakraborty.abhijnan@gmail.com
Joined CSE department in: July 2014

Abhijnan Chakraborty *is a PhD scholar in the Department of Computer Science and Engineering at IIT Kharagpur working under the supervision of Prof. Niloy Ganguly. He is the recipient of Google India PhD Fellowship in Social Computing. Prior to joining PhD, he was working at Microsoft Research (MSR) India for around two years. Abhijnan has obtained M. Tech. in Computer Science and Engineering from IIT Kharagpur in 2012 and B.E. in Information Technology from Jadavpur University in 2009. His research interests broadly lie in Networked Systems, particularly online social networks and mobile networks. He has published papers in top venues like Mobicom, Hypertext etc.*

Supervisor: Prof. Niloy Ganguly

Designing Information Retrieval Systems Optimized to Users' Sampling Strategies

Due to the enormous amount of information being carried over online systems, most users take the help of Information Retrieval (content recommendation, search or ranking) systems to find important information. Because of the churn in information popularity in such systems, the emphasis is on receiving information in real-time. Almost all of the current Information Retrieval (IR) systems emphasize content's "recency" over content's "relevance or long-term popularity", e.g
i. News websites are getting updated almost every hour to show breaking news.
ii. Twitter, Facebook, Google+ are showing trending topics every half-an-hour or so.

A user who is sampling (i.e. logging into) these websites at time t, is only getting top K most popular information, computed based on the instantaneous popularity of all the information at time t. But, there is a limit on the amount of information the user can process (depends on her idle time as well as cognitive limit) e.g. one can read at most 100 news stories a day. There is a notion of timeliness associated with information - one would want to know about some event soon. While looking back at the end of a significant time period (say a week or a month or a year), the user must not miss any information which was really important (or popular) during that period.

Faced with the above constraints, the user is following an ad-hoc sampling rate. As the IR system designers want the users to come back more often on their system to get more eyeballs, the IR systems are becoming more temporal. Their time window of showing top K popular information is thinning gradually forcing the user to sample more. As the sampling rate is approaching the limit for the user, she is feeling exhausted and gradually becoming inactive on that particular system.

In this work, we want to first systematically measure the effect of such frequent information change in the IR systems and investigate efficient sampling strategies for content published in such online systems. Finally, we want to design IR systems which honour individual users sampling strategies, yet maximize coverage over information with "long-term importance" and minimize the delay in getting such information.

Abir De
Email: abir.iitkgp@gmail.com
Joined the department in: July 2012

Abir De *got his B.Tech in Electrical Engineering and M.Tech in Control System Engineering (Dual Degree) both from Dept. of Electrical Engineering of IIT Kharagpur in 2011. He has been a research scholar in the department of Computer Science & Engineering, IIT Kharagpur since 2012. His research interests are in the area of Complex Networks, specifically in Online Social Networks.*

Supervisor: Prof. Niloy Ganguly with collaboration from Prof. Soumen Chakrabarti (IIT Bombay)

Modeling and Learning Influence in Social Networks

The influence that a person has on another person significantly depends on their relationship and the context in which they are. A professor at an university may not have much influence on who her student connects to, on Facebook. But, the student may be highly influenced by her professor when it comes to which piece of literature to read next. Today's vast proliferation of online social networks (OSN) allows us to study such interactions. Here we present two learning models to address the problems of link prediction and understanding opinion propagation in OSNs.

The problem of link prediction (LP) is stated as follows: given a graph, for every vertex in the graph, find vertices to which the given vertex is most likely to form new edges. The problem of link prediction is very important, in the context of social search and recommendation. Our method uses two novel signals to improve accuracy in link prediction. First, we use a co- clustering algorithm to find the underlying communities in the network. We use this information to qualify edges in the graph with a surprise value. This represents how unexpected the edge is in the graph, given the underlying community structure information. Second, we compute a node to node similarity measure which takes into account the local connectivity structure between these nodes. These signals are then used in combination of others as input to a discriminative predictor to estimate likelihoods for future edges. When tested across five diverse datasets, common in link prediction literature, we find our method performs significantly better than standard link
prediction methods.

Today, online social networks constantly bombard users with information. In presence of such a heavy information overload, it becomes critical to understand which pieces of information are getting through and which are ignored. A standard approach, is to model OSN users as actors holding opinions on different topics, which is influenced by their network neighbors. Here we present a novel linear influence model, which unlike existing approaches, makes no assumptions about system stability. At a high level, our method tries to predict the opinion of a user in a social network using a linear combination of opinions of her neighbors, while trying to learn the influence a user has on her neighbors. We tested our approach on three real world datasets; two collected from popular OSNs Twitter and Reddit, and a third one obtained from a live real world experiment conducted in house

with 100 users. Compared to existing apporaches our method has significantly smaller prediction error (smaller by a factor of 2–15)

References :

1. D. Liben-Nowell and J. Kleinberg. *The link prediction problem for social networks*. In Proceedings of CIKM ’03, pages 556–559, New York, NY, USA, 2003. ACM.

2. L. Backstrom and J. Leskovec. *Supervised random walks: predicting and recommending links in social networks*. In Proceedings of WSDM ’11, pages 635–644, New York, NY, USA, 2011. ACM

Anju P J
Email: anjujohnson88@gmail.com
Joined the department in: December 2012

Anju P.J. *received her B.Tech degree in Electronics and Communication Engineering from College of Engineering Chengannur, Cochin University of Science and Technology in 2010, and M.Tech in VLSI Design from Amrita School of Engineering Coimbatore, Amrita Vishwa Vidyapeetham in 2012. During July 2012 to November 2012, she worked as a lecturer in the department of Electronics and Communication Engineering, NIT Calicut. Since November 2012, she is a Research Scholar and a Senior Research Officer in the Department of Computer Science and Engineering,IIT Kharagpur. Her research interests are in the areas of Hardware Security, Low-power VLSI Design and CAD for VLSI Circuits.*

Supervisors: Prof. Rajat Subhra Chakraborty and Prof. Debdeep Mukhopadhyay

Hardware Trojan Evaluation Platform on FPGA

Malicious modification of hardware during design and fabrication have been extensively studied during the last years. HTHs compromises security and integrity of the device either by the leakage of system information or by causing catastrophic system failure. The work investigates the design, detection and prevention of hardware Trojans, in FPGAs. Due to the advancement in technology, FPGAs come up with dynamic partial reconfiguration (DPR) capabilities, which allow hardware modification in the FPGAs already in operation. The malicious hardware modification in the deployed FPGAs emerged as a major security concern and has been given little attention by the security community.

The attack scenario becomes even worse in the case of FPGAs employed in networking application which provides real-time computational capabilities. If the FPGA is remotely accessed over a regular Ethernet connection, some arbitrary modifications on the existing FPGA hardware may insert a back-door into the hardware. We have developed a novel, lightweight and hard-to-detect hardware Trojan which exploits DPR capability and Ethernet connectivity of a FPGA to cause malicious modifications to the existing circuitry. We demonstrated the attack model by inserting a low overhead HTH to cause a fault attack on AES cipher hardware mapped on Xilinx Virtex-5 FPGA platform, leading to the recovery of the secret cipher key. Fault attacks are particularly interesting as they require relatively less computational effort and are easy to launch. The proposed post-deployment “in-field” Trojan insertion strategy evades most traditional static and dynamic Trojan detection techniques. Due to the advancement in technology chips are so complicated and testing them, either physically or logically, is practically impossible. Non-invasive detection methods utilizing side-channel analysis can be to detect the presence of hardware Trojan horses. However, a restrictive mode of DPR can be implemented that can prove effective in preventing Trojan insertion, at the cost of reduced flexibility as security is our major concern.

FPGAs, are widely used in both military and commercial technologies and can contain a large amount of sensitive information. They are widely used in cryptographic devices as accelerated methods can speed the encryption and decryption on FPGAs. So ability to protect the FPGAs from the side-channel

attacks which aim at gaining critical program information stored in very important. This motivates us to study countermeasures against attacks on FPGA based systems and to develop an Evaluation Platform for FPGA hardware Trojans.

Reference

1. Anju P. Johnson, Sayandeep Saha, Rajat Subhra Chakraborty, Debdeep Mukhopadhyay and Sezer Goren, “Fault Attack on AES via Hardware Trojan Insertion by Dynamic Partial Reconfiguration of FPGA over Ethernet”, *Workshop on Embedded Systems Security* (*WESS*, part of *ACM ESWEEK*) 2014, New Delhi, India.

Aritra Hazra
Email: aritrah@cse.iitkgp.ernet.in
Joined the department in: July 2010

Aritra Hazra *received a B.E. degree in Computer Science and Engineering from Jadavpur University, Kolkata in 2006, and an M.S. degree in Computer Science and Engineering from Indian Institute of Technology, Kharagpur in 2010. From July 2006, he worked in several projects of SRIC, IIT Kharagpur, as a Research Consultant. The projects are primarily in the following fields: Design Intent Verification and Coverage Analysis, Power Intent Verification of Power-managed Designs, Platform Architecture Modeling for Exploring Power Management Policies, Functional Reliability Analysis and Reliable Scheduling of Embedded System Controllers. Since July 2010, he has been a research scholar in the department of Computer Science & Engineering in IIT Kharagpur. His research interests are in the areas of Design Verification, Power Intent Verification, Reliability Analysis of Embedded Control Systems. He has published several research papers in various international conferences and journals including a Best Student Paper award in VLSI Design Conference (2010). He has also been awarded with the Microsoft Research (India) Ph.D. Fellowship in the year 2011.*

Supervisors: Prof. Pallab Dasgupta and Prof. Partha Pratim Chakrabarti

Formal Methods for Architectural Power Intent Verification and Functional Reliability Analysis

The increasing complexity and safety-criticality of modern-day systems has introduced the need for comprehensive validation and provable safety assurance of these designs based on formal analysis. During the development phase, the designers need to consider four critical aspects of design, namely – functional correctness, end-to-end timing, power performance and functional reliability. Formal methods have been traditionally confined to ensuring functional correctness of a system using methods such as model checking and design intent verification. Recent research also focuses on guaranteeing stringent timing requirements of a system by choosing the timing layout for the constituent components.

However, functional correctness is only one of many aspects in modern engineering design. Performance parameters such as power, reliability etc. have become equally dominant aspects in determining the acceptability of a design. This work is an enabler for early-stage formal certification of performance requirements, such as power intent and functional reliability. In particular, we have the following contributions:

Architectural Power Intent Validation: The rapid increase in design complexity and a stringent low-power budget make the power management schemes highly sophisticated. The logic behind these strategies is decided at the architectural level. Today there is a disconnection between the high-level architectural power management strategies which relates multiple power domains and the low-level assertions for controlling individual power domains. This poses two challenges in validating the power performance, namely:

- Verifying that the architectural power management strategy has been correctly implemented in the power-managed designs, and
- Estimating the power performance of an architectural power management strategy depending on

typical usage profiles.

The first aspect is addressed in our proposed verification framework, based on our proposed tool, named POWER-TRUCTOR, that attempts to bridge the disconnect between high-level properties capturing the architectural power management strategy and the implementation of the power management control logic using low-level per-domain control signals. The second aspect is addressed by our proposed tool, named POWER- SIM, while deciding the power architecture of the integrated circuit and converging into the best power domain partitions before the power management logic is laid out.

Functional Reliability Analysis: Reliability is one of the critical factors in the development of safety-critical embedded designs such as automotive and avionic control systems, nuclear reactors, navigation / signalling systems etc. In the foreseeable future, reliability guarantees will become an integral part of safety-critical specifications, and will need to be formally specified and certified upfront in the design flow. This introduces the following three facets in reliability analysis:

• Formally expressing the functional reliability requirements leveraging the spatial and temporal redundancy provisions,
• Analyzing the system reliability (at an early-stage) as entailed by the reliability specifications of its constituent components, and
• Deriving the reliability gap from the given reliability choices of component-level properties and indicating the solution space to bridge the gap. To address the above objectives, we provide novel formalisms to overlay reliability specifications on the functionality of a design and propose suitable methods to compute system reliability. Further, this work introduces the formal notion of reliability gap and proposes a divide-and-conquer algorithm to bridge the same.

Aritra Mahapatra
Email: aritra.mhp@gmail.com
Joined the department in: December 2014

Aritra Mahapatra *received his B. Tech in Information Technology from Govt. College of Engg. & Ceramic Technology and his M. Tech in Information Technology from University of Calcutta. He is now a Senior Research Fellow in a DST Project in IIEST, Shibpur. His research interests are Bio-Informatics, Phylogeny, Bio-medical Engineering.*

Supervisors: Prof. Jayanta Mukhopadhyay

My research is on the Evolution of Exon-Introns in gene. Exon and Introns are the two parts of a gene. Exons are involved to code for protein. Intron (the term intron is derived from intragenic region) is the intermediate part of exon which does not code for protein. An intron is removed by RNA splicing while the final mature RNA product of a gene is being generated. After removed the intron, the exon sequences are joined together in the final mature RNA.

In the case of intron, there are some questions. Firstly, what are the roles of an intron in gene? Secondly, what are the roles of intron in the evolution of a gene? Thirdly, what is the origin of intron? What information stores in the sequences of intron? Finally, from the axon-intron gene sequences can we derive the ancestor of the species?

Exon insertions and duplications, two major mechanisms of exon shuffling, are shown to involve modules that have introns of the same phase class at both their S- and 3'-ends. At the sites of intronic recombinations exon insertions and duplications create new introns which belong to the same phase class as the recipient introns. As a consequence of repeated exon insertions and exon duplications introns of a single phase class predominate in the resulting genes, i.e. gene assembly by exon shuffling is reflected both by this nonrandom intron phase usage and by the correlation between the domain organization of the proteins and exon-intron organization of their genes.

Ayan Das
Email: ayandas84@gmail.com
Joined the department in: July 2013

Ayan Das *received his B.Tech. degree in Computer Science and Engineering from National Institute of Technology, Durgapur in 2008. From July 2008 till July 2011, he worked in Tata Consultancy Services, Kolkata, as a Systems Engineer. He received his M.Tech. degree from in Computer Science and Engineering from Indian Institute of Technology, Kharagpur in 2013. Since July 2013, he has been a research scholar in the department of Computer Science and Engineering in IIT Kharagpur. His research interests are in the areas of Machine Learning, Convex Optimization and Natural Language Processing.*

Supervisor: Prof. Sourangshu Bhattacharya

Distributed Regularized Loss Minimization

Training machine learning algorithms on massive datasets require huge amount of computational resources. Mouse visual cortex data hosted by Open Connectome Project 10 terabyte dataset has a size of 10 terabyte, Image-net database which is a repository of images from the web has about 14 million images (instances) organized into one of 20,000 words (class-labels) from the word-nethierarchy and Image-net database which is a repository of images from the web has about 14 million images (instances) organized into one of 20,000 words (class-labels) from the word-net hierarchy (1.2 terabyte) are some examples of extremely large datasets. Sometimes accumulation of an entire dataset in a centralized processing unit is prohibited due to, for example, communication complexity, scalability, or privacy reasons.

For many machine learning models (SVM, Conditional Maxent, Linear Regression etc.) training is done through regularized loss minimization. Our goal is to develop algorithms to train supervised learning models in distributed manner, when training data are distributed across different nodes.

To accomplish this goal, the regularized loss minimization problem is cast as a set of convex optimization subproblems (one per site) with consensus constraints on the variables. We have observed that, although, simple averaging of the parameters learnt at different sites shows good performance, the accuracy drops with increase in number of sites if the number of training points remains constant. This fact motivated us to to solve weighted parameter averaging.

We use a master-slave architecture to solve this problem where all the sites containing the training data(slave) are connected to the central computer(master). Given this distributed setting, alternating direction method of multipliers provides a framework for implementation of the loss minimization algorithms such that distributed training algorithms are implemented without exchanging trining data among nodes. Currently, Our aim is to learn an optimal weight to each SVM parameter trained locally at different sites such that their weighted sum approximates the single SVM parameter, obtained by training SVM locally with all the datapoints. This substantially reduces the amount of data exchange among the nodes. Since, the size of weight vector is equal to the number of sites in which the data is distributed, which is several orders smaller than the size of the SVM parameters or the total number of training data points.

References

[1] Stephen Boyd, Neal Parikh, Eric Chu, Borja Peleato, and Jonathan Eckstein. Distributed optimization and statistical learning via the alternating direction method of multipliers. *Found. Trends Mach. Learn.*, 3(1):1–122, January 2011.

[2] Michael Grant and Stephen Boyd. Graph implementations for nonsmooth convex programs. In V. Blondel, S. Boyd, and H. Kimura, editors, *Recent Advances in Learning and Control*, Lecture Notes in Control and Information Sciences, pages 95–110. Springer-Verlag Limited, 2008. http://stanford.edu/~boyd/graph_dcp.html.

[3] Gideon Mann, Ryan McDonald, Mehryar Mohri, Nathan Silberman, and Dan Walker. Efficient large-scale distributed training of conditional maximum entropy models. In Y. Bengio, D. Schuurmans, J. Lafferty, C. K. I. Williams, and A. Culotta, editors, *Advances in Neural Information Processing Systems 22*, pages 1231–1239. 2009.

Barnali Das
Email: bdbarnalidas@gmail.com
Joined the department in: July 2014

Barnali Das *has done her B.Tech in Computer Science & Engineering from St. Thomas' College of Engineering & Technology, Kolkata in 2012. She received her M.E. degree in Information Technology from Indian Institute of Engineering Science and Technology, Shibpur in 2014. Her research interest includes the design of Constrained Brownian Dynamics Force-Field to Simulate Bacterium Escherichia coli.*

Supervisor: Dr. Pralay Mitra

Designing Constrained Brownian Dynamics Force-Field to Simulate Bacterium *Escherichia coli*

Designing and simulating cellular models have been a challenging task in the field of computational cellular biology. Though a multitude of operations take place in a cell simultaneously, there are no universal empirical rules governing these operations. As a result, certain randomness exists in the way of execution of the processes within a cell. The biomolecules moving inside a cell do not follow different trajectories for its function. All biological components have well defined structure and function i.e., nothing is random when spoken of the components. So, there must be a rule or a protocol following which, the diverse processes occur in a cell. Each molecule in a cell follows a particular trajectory for its function i.e., the movement of a molecule inside the cell is mostly deterministic and constrained. Initially, without any constraints the whole cell system can be thought of having pure Brownian motions (random motions). The main objective of our research is to design a whole cell simulation force-field using Constrained Brownian Dynamics (CBD) for bacterium *Escherichia coli* (E. coli) which will be the proof of the deterministic constrained motion of the molecules within the cell. This will ultimately lead to the design of the whole cell model.

Bijju Kranthi Veduruparthi
Email: bijjuair@gmail.com
Joined the department in: July 2013

Bijju Kranthi *received a B.Tech. Degree in Electronics & Communications Engineering from Vaagdevi College of Engineering, Warangal, Andhra Pradesh in 2007 and an M.Tech degree in Image Processing & Embedded Systems from the Department of Electronics & Electrical Communications Engineering, IIT Kharagpur. From Sept 2007 till Nov 2009, he worked with IBM India Pvt. Ltd as a Software Developer in the Telecom domain and from July 2012 to April 2013 he worked in Memory Architecture Validation at Nvidia Graphics, Bangalore. Since July 2013, he has been a research scholar in the Department of Computer Science & Engineering in IIT Kharagpur. His research interests are in the areas of Computer Vision,Medical Image Processing and Pattern Recognition.*

Supervisors:Prof. Jayanta Mukhopadhyay and Prof. Partha Pratim Das

Lung Tumor Analysis on CBCT for Radiation Treatment Planning

Lung Tumor Volume estimation on imaging modalities is required to assess the extent of the tumor for diagnosis. In this document we address tumor volume estimation in Cone-Bean Computed Tomography (CBCT) images. Given a doctor dilineation in the week zero of Radiation Treatment Planning, we wish to estimate the tumor areas which the doctor might have missed. Additionally we wish to estimate the tumor volume change on CBCT volumes in subsequent weeks. Using serial on-treatment cone beam CT scans (CBCT), we will analyze the early changes in the CBCT images and predict the likelihood of response of the tumor based on the early changes. Classification approach to delineate tumor is not helpful due to high randomness of pixel intensities in tumor and non-tumor regions. To solve the segmentation problem we take the help of PET-CT along with CBCT. An image registration approach is used to help solve the segmentation problem.

Image Registration

PET-CT are registered with the CBCT using Mutual Information based techniques. Since tumor is easily identifiable in PET-CT, the registration can help in identifying and delineating tumor in CBCT images. A two step registration process is followed for global and local registration using rigid and deformable registration respectively. The deformable registration has been implemented using a viscous fluid model. Once the images are registered, a simple subtraction of the CBCT images of various weeks can reveal a lot about the tumor growth and reduction. These changes are analyzed to identify the radiation treatment planning that had been done on the patient. Better and more focused radiation treatment may be proposed based on the analysis of the tumor regions.

Bruto da Costa António Anastásio
E-mail: bruto@cse.iitkgp.ernet.in
Joined the department in: July 2014

António Anastásio Bruto da Costa *received his Bachelor of Engineering degree in Computer Engineering from Goa Engineering College, Goa University, Goa in 2010, and an M.Tech. degree in Computer Science and Engineering from Indian Institute of Technology, Kharagpur in 2014. He holds the State Gold Medal (B.E, 2010) and was awarded the Institute Silver Medal (M.Tech, 2014). From July 2010 to May 2012, he worked as a Software Engineer at Persistent Systems, Verna - Goa. In January 2014, he worked as an Intern at Texas Instruments, Bangalore. Since July 2014, he has been a research scholar in the department of Computer Science & Engineering in IIT Kharagpur. His research interests are in the areas of Formal Verification of Hybrid Systems.*

Supervisors: Prof. Pallab Dasgupta (IIT-Kharagpur) and Prof. Goran Frehse (Verimag – France)

Formal Methods for Feature Based Analysis and Equivalence checking of Hybrid Automata.

Equivalence checking for finite state systems is well studied, and many algorithms exist that can determine whether or not two finite state systems are equivalent. Due to the inherent undecidability in answering questions about infinite state systems, analysing them is very challenging. An abstraction of Infinite state systems that has been found useful is that of Hybrid Automata. Hybrid Automata allow for modelling both discrete and continuous behaviours that describe the operation of complex systems.

Many methods exist for checking equivalence between two Finite State Systems. However, for infinite state systems, this traditional crude definition of equivalence is too constrained. A more effective equivalence definition is one that is best expressed in terms of *features* or behavioural signatures of the infinite state systems. In this regard, we define the notion of a feature which is a sequential expression (as an assertion), over predicates over real variable, the dense temporal domain, and with the use of local variables (as used in SVA); and a computation over feature local variables and system variables. The sequential expression, allows us to express the intended behaviour of interest as a sequence of events, and associated with the behaviour is the computation. Since the system can exhibit behaviour along various execution paths, the computation yields a range of values, which we call the feature's signature.

We propose that behavioural aspects (feature signature's) used for feature comparison can be expressed as a linear combination of state variables. For a given Hybrid Automaton, the range of values taken on by a specific feature aspect can be obtained by observing the state space of the Hybrid System reachable from an initial state.

However, due to the level of abstraction of the Hybrid Automaton, feature based analysis cannot be directly applied. More so, neither can we directly apply traditional reachability analysis techniques for our purposes.

In addition to this, Hybrid Automata model systems which have complex behaviours. However limited, techniques to model constant and affine dynamics are used in most reachability analysis tools.

For non-linear systems these tools either are unequipped to handle, or do not scale well.

This work formalizes the notion of *Feature based Reachability Analysis of Hybrid Systems* and builds feature driven transformations to prepare the given Hybrid Automata for feature based analysis. It also works to understand which states and execution paths are irrelevant to analysis, and may therefore be pruned. Finally the work also pushes towards building scalable algorithms for analysing Hybrid Systems with combinations of linear, affine and non-linear dynamics.

Debapriya Basu Roy
E-mail: dbroy24@gmail.com
Joined the department in: December 2011

Debapriya Basu Roy received a B.Tech. degree in Electronics & Communication Engineering from RCC Institute of Information Technology, Kolkata in 2011. Since December 2011, he has been a research scholar in the department of Computer Science & Engineering in IIT Kharagpur. He has completed his MS and currently enrolled as joint MS-PhD scholar. His research interests are in the areas of Cryptography and VLSI design, Hardware Security, FPGA based system design, Side Channel Analysis and Elliptic curves.

Supervisors: Prof. Debdeep Mukhopadhyay

Indigenous Design Methodologies for Elliptic Curve Cryptography with Inherent Side Channel Countermeasure

With the increase of sensitive information in the Internet, security is becoming a very important aspect of web applications. Applications like e-commerce and net-banking require transfer of sensitive information via Internet and hence needs to be protected. Cryptography provides us the means of protecting these sensitive information by producing efficient algorithms for encryption, authentication and verifications. Generally cryptographic algorithms can be broadly classified into two groups: symmetric key and asymmetric key cryptography. The most popular asymmetric key algorithms are RSA and ECC. RSA, introduced by Ron Rivest, Adi Shamir and Leonard Adleman in 1977, has been widely used in various applications. However, an RSA algorithm requires around 1024-2048 long keys and is extremely resource hungry. On the other side, Elliptic Curve Cryptography (ECC) provides same security with significantly short keys. Hence, security protocols based on elliptic curves are gradually becoming the standard for a wide range of applications. However, the intensive mathematical computations involved in elliptic curve cryptography (ECC), creates performance bottlenecks for a number of applications involving web servers, cloud computing infrastructures, and data centers. Operations in ECC involves finite field arithmetic which is time consuming to implement in software, unless the processor is equipped with finite field instructions. A popular alternative is to provide a dedicated hardware accelerator for ECC operations which will work as a peripheral device of the processor to accelerate ECC based protocols.

NIST (National Institute of Standards and Technology) has proposed many curves which are used as standard of ECC [18]. These curves are more efficient than other curves when implemented on ASIC or FPGAs as they take less gate count or logic slices but provide high throughput performance . These curves are widely used and has been adopted as standard in various security suits like OpenSSL.

The curves, specified by NIST, tries to ensure that elliptic-curve discrete-logarithm problem (ECDLP) is difficult so that the an adversary can not obtain a user’s private key from his public key. But, though this curves maintains the intractability of ECDLP, it is not sufficient to provide ECC security. Strangely, it has been found that most of the standard curves of NIST are susceptible to such kind of

security threat and are actually unsafe for secure communication.

Apart from standard cryptanalysis technique, ECC can also be vulnerable against side channel attacks. Side channel attack on a cryptographic system exploits vulnerabilities of the implementation of the crypto-system. This attack uses any unintended source of information leakage (power, time, electro-magnetic radiation etc.) and tries to retrieve the secret information. To prevent side channel attacks, the design need to be equipped with side channel countermeasure, either algorithmic or circuit level. There are some countermeasures which are generic and can be used for any crypto- algorithm like private circuit, dual pre-charge logic e.t.c. On the other hand, there are some countermeasures which are more suitable for specific type of algorithm. For example, masking, DRECON are more suitable for symmetric key algorithms (block ciphers). Similarly for ECC, researchers have proposed various countermeasure techniques like point and scalar blinding, point coordinate randomization, isomorphism e.t.c. However, no study has been done to analyze the nature of the curves on the side channel security.

The aim of is to achieve the following goals:

1. We want to design efficient hardware architecture for the existing non-NIST curves which are secure against standard ECC security threats. The objective is to compute the cost in terms of area and performance for deporting from vulnerable NIST curves to secure non-NIST curves.

2. We also aim to design new curves which provides similar efficiency like NIST curves in hardware result but also secure against standard ECC and ECDLP security threats. The objective is to propose new standard of ECC which is both secure and efficient.

3. Lastly, we want to analyze side channel security in terms of elliptic curve parameters. The objective is to design elliptic curves which are inherently resistant against side channel security. This will reduces the overhead, which are generally incorporated in the design due to the expensive side channel countermeasures.

Debashis Mukherjee
Email: debashis.mukherjee@cse.iitkgp.ernet.in
Joined Department in: December 2014

Debashis Mukherjee *is pursuing research for his PhD degree in the broad area of "program analysis and testing using machine learning approaches" in software engineering. Earlier he had worked in the area of image processing and pattern recognition in his M.Tech degree in Computer Technology at Jadavpur University and in fellowship under DieTY project in Dept. of C.S.E in J.U. in 2013, and in the past in area of geometric modeling for computer aided design in his M.Sc.(engg.) degree in Mech. Engg. in Indian Institute of Science in 1998. Debashis had M.Tech in Computer Technology from Jadavpur University in 2013, M.Sc.(engg.) in Mech. Engg. from IISc Bangalore in 1998, and B.M.E. in Mech. Engg. from Jadavpur University in 1996. Debashis had employment experience of nearly 12 years, as consultant, system analyst, etc. in the most recent with Cognizant technology solutions Ltd., IBM India pvt. Ltd. in Kolkata.*

Supervisor:Prof. Rajib Mall

Debashis is currently working on a data and control dependency based test coverage metric that is being computed based on Program Dependence Graph (PDG).

Dhiman Saha
Crypto Research Lab
Email: crypto@dhimans.in
Joined the department in: April 2012

Dhiman Saha *was born and brought up in the north-eastern hilly state of Tripura. He graduated from National Institute of Technology, Agartala in Computer Science and Engineering in 2006. He received his MS degree from the Department of Computer Science & Engineering, IIT Kharagpur in 2010. Between 2010 and 2012 he worked in Atrenta India Pvt. Ltd and Interra Systems India Pvt. Ltd. in the capacity of a Senior Software Engineer. He joined the department back in April 2012 for his PhD program. He is a computer geek and loves programming and social networking and is also a passionate photographer. His current research interests revolve around fault attacks, hash functions and authenticated encryption. He can be reached at* ***http://www.dhimans.in****.and* ***http://de.ci.phe.red***

Supervisor: Prof. Dipanwita Roy Chowdhury

Cryptanalysis of Hash Functions and Authenticated Encryption Schemes

Cryptography encompasses a plethora of things that determine how information is securely transmitted over an un-trusted network. Certain texts refer to cryptology as the study of cryptography and cryptanalysis, where the later consists of techniques used to analyze a cryptosystem so as to gain some useful information which may help in breaking it. Thus, here we are both concerned about making and breaking a cryptosystem. This particular property makes this field of research interesting and challenging. This has also had led to the constructive development of cryptography from ancient times when constructions were based on unproven assumptions to the age of modern cryptography which is heavily based on mathematical theory and the theory of computer science. Modern cryptography can be broadly classified into two streams viz., symmetric-key, where the same key is used to encrypt and decrypt and asymmetric key where the encryption and decryption keys are different. This work primarily focuses on symmetric-key constructions and analysis of their properties.

Cryptographic hash functions play a major role in providing data integrity and authenticity. These one-way functions essentially operate on arbitrary length input and provide a fixed length hash/digest as output. In the last 5 years, the cryptographic community has seen remarkable progress in the design and analysis of hash functions and the credit mainly goes to the introduction of the Secure Hash Algorithm-3 (SHA-3) contest [1] by NIST following the concerns over the security flaws in SHA-1 and SHA-2. The primary outcome of the SHA-3 contest was the submission of innovative designs for compression functions and new modes of operation. The contest declared 5 finalists and in October 2012 announced KECCAK [2] as the next SHA-3 standard. This work focuses on the cryptanalysis of the new generation hash functions with special attention to KECCAK. This includes finding collisions, pre-images as well as devising distinguishers.

Cryptography has been successful in addressing the issues of providing privacy and

integrity/authenticity *separately* by providing constructions that have sound theoretical analysis and at the same time are highly optimized for both software & hardware implementations. Authenticated encryption aims at combining the goals of privacy and authenticity under a single crypto-primitive to achieve both, preferably, at the cost of one. During the last decade, authenticated encryption has received considerable attention from the crypto community. This has also resulted in the evolution of the field from the initial realms of using just generic compositions to the present day where standalone algorithms are being proposed. The announcement of **CAESAR**: **C**ompetition for **A**uthenticated **E**ncryption: **S**ecurity, **A**pplicability, and **R**obustness [3] in 2013, has laid the foundation for further research in this domain. This precludes the need for analyzing the submissions to the CAESAR competition. In this work, we try to concentrate on analysis of the state-of-the-art authenticated encryption schemes and evaluate them in the light of both theoretical and side-channel cryptanalysis.

References:

[1] National Institute of Standards and Technology. *Announcing Request for Candidate Algorithm Nominations for a New Cryptographic Hash Algorithm (SHA-3) Family*.
Federal Register, 27(212):62212–62220, November 2007.
Available at http://csrc.nist.gov/groups/ST/hash/documents/FR_Notice_Nov07.pdf

[2] Guido Bertoni, Joan Daemen, Michael Peeters, and Gilles Van Assche.
The KECCAK SHA-3 Submission. Submission to NIST (Round 3), 2011.
Available at http://keccak.noekeon.org/Keccak-submission-3.pdf.

[3] CAESAR: Competition for Authenticated Encryption: Security, Applicability and Robustness (April 2013)
[4] Available at http://competitions.cr.yp.to/caesar.html

Durga Prasad Sahoo
Email: dpsahoo.cs@gmail.com
Joined the department in: December 2011

Durga Prasad Sahoo *received B.Sc. degree in Computer Science from Ramakrishna Mission Residential College, University of Calcutta, Kolkata in 2007; M.Sc. degree in Computer and Information Science from University of Calcutta, Kolkata in 2009 and M.Tech. degree in Computer Science from University of Calcutta, Kolkata in 2011. From August 2011 till December 20011, he worked in Asutosh College, Kolkata, as a guest lecturer. Since December 2011, he has been a research scholar in the department of Computer Science & Engineering in IIT Kharagpur. His research interests are in the areas of Hardware Security and Applied Cryptography.*

Supervisors: Prof. Rajat Subhra Chakraborty and Prof. Debdeep Mukhopadhyay

Design and Analysis of Secure Physically Unclonable Functions

Counterfeiting of hardware devices and its impact on economy has become a big concern to modern society. The most well-known aspect of counterfeiting is product cloning. In order to deal with this aspect of counterfeiting, a secret unclonable identifier is required. The idea of using intrinsic random physical features to identify objects has led to the development of the concept of *Physically Unclonable Function* (PUF). The fact that PUFs are unclonable implies that they can be used for anti-counterfeiting purposes. When PUFs are used for the detection of the authenticity of a product, a physical property of the PUF is measured, translated into a bit string and verified. The physical unclonability of PUFs prevents building of a similar physical structure that upon interrogation produces a similar bit string that would pass the verification test as the original one.

However, recent studies on PUFs have challenged claims of unclonability by demonstrating that the behavior of PUFs, especially those implemented as solid-state electronic circuits, can be modeled by using machine learning techniques such as *logistic regression*, *perceptron learning*, *support vector machine*, etc. Most common type of PUFs those are candidate for machine learning based attack are *Ring-Oscillator PUFs* and *Arbiter PUFs*. My research deals with the design of lightweight and secure PUF design. We have proposed a new PUF design paradigm for FPGA platform, known as Composite PUF, which can be used to design a new PUF using the existing primitive PUF designs. This design approach can be used to enhance the quality as well as the security of the resultant PUF. It is published in IEEE HOST-2014. In addition, we have proposed cryptanalysis attack on Enhance Ring Oscillator PUF and it is accepted in DATE-2015. We are also working on the cryptanalysis of Lightweight Secure PUF (LSPUF) designs.

Jimmy Jose
Email: jimmy@cse.iitkgp.ernet.in, jimmy.nitc@gmail.com
Joined the department in: July 2012

Jimmy Jose *received his B Tech in Computer Science and Engineering from University of Kannur, Kerala in 2001 and M Tech in Computer Science from University of Kerala in 2006. He worked as Lecturer in Computer Science at University Institute of Technology, University of Kerala (January 2002 - June 2003), Rajagiri School of Engineering and Technology, Kochi (June 2003-January 2004), and College of Engineering Munnar (Jan 2004-May 2007). He worked in NIT Trichy as Assistant Professor from May 2007 to December 2007 and joined NIT Calicut in December 2007 and continues to be part of the institute. He joined the Department of Computer Science & Engineering in IIT Kharagpur as research scholar in July 2012. His research interests are in the areas of Cryptography and Security.*

Supervisor: Prof. Dipanwita Roychaudhury

Study of Cellular Automata and its Application to Stream Cipher

Stream Cipher is one of the most important branches in symmetric-key cryptography for it is highly suitable for resource-constrained systems. The goal of a stream cipher design is that it must provide high-speed encryption and less design overhead in comparison with block ciphers. A number of stream ciphers have been reported in literature including ciphers in eStream project among which some are hardware efficient whereas some are software efficient. On the other hand, stream ciphers with the goal of receiving higher throughput than the eStream ciphers are also reported in literature. This PhD work aims to study Cellular Automata (CA) and how CA can be used as effective cryptographic primitive in stream ciphers.

One of the methods of cryptanalysis on stream ciphers is the fault attack. These types of attacks were later improved by algebraic techniques. Trivium, one of the finalists in eStream project, is also susceptible to fault attack. The attack exploits the fact that the non-linearisation process of Trivium is very slow. Our work shows that fault attacks against stream ciphers can be prevented by using CA as a cryptographic primitive. Our current work focuses on how the neighbourhood size influences the cryptographic suitability of Cellular Automata.

Joy Chandra Mukherjee
Email: joy.cs@cse.iitkgp.ernet.in, mjoy1982@gmail.com
Joined the department in: July 2011

Joy Chandra Mukherjee *received a B.Tech. degree in Computer Science and Engineering from Bengal Institute of Technology, Kolkata in 2004. From November 2004 till September 2007, he worked in CTS, Kolkata as an Associate. Since October 2007 to October 2008, he worked as an Assistant Systems Engineer in TCS, Kolkata. He received an M.Tech. degree in Computer Science and Engineering from Indian Institute of Technology, Kharagpur in 2011. Since July 2011, he has been a research scholar in the Department of Computer Science & Engineering in Indian Institute of Technology, Kharagpur. His research interests are in Mobile Computing and Distributed Algorithms.*

Supervisor: Prof. Arobinda Gupta

Scheduling in Large Scale Mobile Networks

In our research, we primarily focus on understanding the dynamics of mobile entities in large scale networks and realize the design of distributed scheduling algorithms for (i) Vehicular ad hoc networks, and (ii) Smart Grid networks.

Scheduling of Events in VANETs: Many applications have been proposed for use in vehicular environments such as vehicular ad-hoc networks (VANET) for different purposes such as safety, convenience, financial, and navigational aid etc.. Typically, such environments consist of moving vehicles and roadside infrastructure (road-side units or RSUs), with potential communication both between vehicles and between a vehicle and an RSU. The RSUs are usually connected to the internet through some backbone network. Many of these applications require different types of information to flow across the environment from places where the information originates to vehicles that are interested in them. For example, an office-goer may want to know about traffic conditions at different parts of the city on his/her way to office or about available parking spots close to the office, an ambulance driver may look up availability in a nearby hospital, a tourist bus may want to know the weather condition at the tourist spots etc.. These information are useful to the vehicles only when they are available in time. Also, the information required by a vehicle should be delivered to the vehicle on its way, without requiring the vehicle to deviate from its route. Such information access and delivery in time and in place in a vehicular environment is an interesting problem. We investigate the use of a publish-subscribe based framework using RSUs for efficient delivery of such information.

A publish-subscribe communication system has been viewed as a suitable communication framework for information dissemination where the underlying network is constantly changing, and the application interactions are asynchronous in nature. It connects together information providers and consumers, which are vehicles in our case, by delivering events from a publisher to all the interested subscribers. A user expresses his/her interest in an event, or a pattern of events by submitting a predicate defined on the event contents, called the user's subscription. When a new event is generated and published to the system, the publish-subscribe infrastructure is responsible for checking the event against all current subscriptions and delivering it efficiently and reliably to all users whose subscriptions match the event.

Using the publish-subscribe framework for event notification in vehicular environments would require vehicles to subscribe to specific types of events through roadside units to a service provider; the events are also reported to the service provider. The service provider delivers the events to the subscribed vehicles within the validity periods of both the subscriptions and the events through roadside units placed along the trajectory of a vehicle. We have formulated the event placement problem as an optimization problem that will optimize the cost of placing events in the RSUs, and we are currently working on an algorithm to solve the problem.

Scheduling the charging behavior of Electric Vehicles in Smart Grid Networks: During the last few decades, the continuous depletion of oil reserves and environmental impacts (CO_2 emissions) due to fossil fuels used by internal combustion engines have led to renewed interest in the potential use of electric vehicles (EVs).

If a fleet of EVs can be managed appropriately, a large share of such vehicles can also become an asset for an electric power grid: electrical load can be shifted in time, and excessive EV battery energy could be fed back into the electrical grid. This concept is known as vehicle-to-grid (V2G) technology. For example, in grids with high degrees of fluctuations and renewable power sources such as wind or solar power, the demand-response potential of an EV fleet can be exploited to enhance grid stability. When the supply of energy is low, EV battery charging may be delayed or stopped. Conversely, when energy is abundant, charging takes place at a higher pace.

To integrate a fleet of EVs into the electrical grid, intelligence is needed to optimize and control the charging of EV batteries. In particular, the following issues must be addressed by an EV aggregator or Electric Vehicle Virtual Power Plant (EV-VPP)): (i) deliver sufficient energy to vehicles, (ii) minimize the cost of charging, (iii) respect grid constraints. The EV-VPP thus needs to mediate between the energy suppliers (generation) and consumers (EV charging). Based on usage predictions, the charging behavior of EVs can be anticipated, optimized, and aligned with forecasts of fluctuating energy production. As part of our future work, we have planned to work on the charge scheduling problem of electric vehicles in smart grid network.

Kamalesh Ghosh
Email: kamalesh.ghosh.iitkgp@gmail.com
Joined the department in: July 2009

Kamalesh Ghosh *received a B.Tech. (Hons) degree in Computer Science and Engineering from IIT Kharagpur in 1998. From July 1998 to April 1999 he worked as a software engineer with Wipro Infotech Ltd. (Bangalore) on e-commerce products. From April 1999 to Dec 2000, he worked as a senior software engineer at Delsoft India Pvt. Ltd. (Noida), an Electronic Design Automation (EDA) company. From Jan 2001 to Oct 2004 he worked as senior R&D engineer at Synopsys Inc. (Marlboro, MA) on verification tools for VLSI design. From Nov 2004 to Nov 2007 he worked at Synopsys India Pvt. Ltd. (Bangalore) as senior R&D Engineer, continuing in the same area of work. From Dec. 2007 till now, he has been working as a Research Consultant in the department of Computer Science and Engineering at IIT Kharagpur, pursuing a Ph.D. degree simultaneously. His research interests are in the area of Artificial Intelligence and Formal Verification with particular focus on application to component based design of safety critical real-time systems.*

Supervisor: Prof. Pallab Dasgupta

Formal Methods for Top-Down Component Based

Component based Software Engineering (CBSE) is a very popular paradigm in modern software engineering. The CBSE approach focuses on building software systems with commercial-off-the-shelf (COTS) components or existing in-house components rather than ground-up development. When safety critical systems with real-time requirements (e.g. automotive) are built using this paradigm, sources of failures can be many. For example – the timing and logical properties of the built system are inherently difficult to predict or verify. Our work is focused on finding novel techniques that may help in closing some of these sources of failure.

Conceptually, we visualize three abstract layers across which the design and implementation of the system is distributed. The topmost layer is named the Feature Layer in which the requirements of the built system are captured from a user's perspective. This layer is the most idyllic view of the system which will just list desirable features and have no connection to lower level concerns. The second layer, named Interaction Layer, is a cluster of various "subsystems" which coalesce together to build up the system. Each "subsystem" may be thought of as a component in our CBSD paradigm, which is being bought as a COTS component or developed independently in-house by the manufacturer, e.g. the braking subsystem or the powertrain subsystem for a car. Though this layer is still not giving a complete picture of the working of the whole system, it is more grounded towards reality and detailed. The lowermost layer, called the Component Layer, is where the real implementation is captured. This 3-layer visualization mimics the phases in the design of a real-life system quite realistically. Our work is entirely focused on the verification problem across the top two layers in this conceptual framework.

In our first problem, the interaction layer specifications are formally written as sets of preconditions and postconditions. Each precondition-postcondition pair is called an action and either defines what the controller must do when the preconditions hold or defines what the environment (driver, road etc.) may do if it chooses to. In the former case the actions are called control actions while in the later case we call them environment actions. Thus our formalism includes the operational environment and control specification of the system as its core elements. The feature layer is simply

modeled (for now) as a set of logical statements which indicate desired properties (checks) for the system. The control should never allow any of these to be violated (intermittent violations are allowed, but the control should never allow the system to sustain such a violated state). We model the environment and control as two adversaries in a game-like scenario. The environment makes moves to violate a property representing a vehicle feature requirement, while the control interrupts at every move of the environment and executes pre-specified actions. The property is verified if the environment has no winning strategy. This model allows us to do a logical evaluation of the software control logic at a stage when few low level details are available. The benefit of this analysis is that we may detect “logic bombs” at a very early stage of design.

Further exploiting the opportunities implicit to our base formalism we aim to catch contradictions or inconsistencies in the specification through automatic detection of loops consisting of control actions. Loops in the high level specification of a control naturally arouse suspicion as it can be indicative of contradictions. We have worked on algorithms to efficiently discover such implicit loops in action-based specifications.

Specifications for real-time reactive systems often need to refer to numerical value of physical quantities such as speed, acceleration etc. Any formalism without this basic expressive power can be considered too limited for practical use. However, allowing for expressions with numerical variables under standard operations like addition, multiplication etc. causes the verification problem to become undecidable and completely unyielding to any practical methods of rigorous verification. Our research explores limited enhancements in expressive power in the numeric domain to find a good trade-off between expressive power and ease of verification. As an outcome of our research, we have been able to build a tool with a good balance of such tradeoffs. The input language of our tool is an adaptation of the numeric extensions of the Problem Domain Definition Language (PDDL), though our solution methods are entirely new.

As a further addition, we explore methods to incorporate temporal specifications (such as LTL) for control and environment in our formalism. We have built a tool which gives scope for incorporating this, and also has the ability of combining it with other enhancements, such as the numeric extensions mentioned above, in a single tool.

[*This research is supported by a grant from General Motors under the GM-IIT Kharagpur Collaborative Research Lab.*]

Koustav Rudra
Email: koustav.rudra@cse.iitkgp.ernet.in, krudra5@gmail.com
Joined the department in: July 2013

Koustav Rudra *received B.E. degree in Computer Science and Technology from Bengal Engineering and Science University in 2011 and M.Tech degree in Computer Science and Engineering from Indian Institute of Technology, Kharagpur in July, 2013. Since then, he has been a research scholar in this Department and his research interests are in the areas of Social Networking, Natural Language Processing.*

Supervisor: Prof. Niloy Ganguly

Online social networks (OSNs) like Twitter, Facebook etc. are currently important sources of information on the web. They are not only used to keep in touch with friends but also to gather information on various topics and current events. Especially, Twitter is increasingly being used to gather real time information on events happening "now", including disasters, emergency situations, political/social movements, and so on. In fact, recent research shows that Twitter reports same events as news media sites (e.g. Newswire), and even captures many minor events which are ignored by news providers.

In particular, recent studies have shown the utility of online social media as a sentinel in emergency situations. During crisis events -- which include natural emergencies such as earthquakes, tsunami, cyclones as well as man-made emergencies such as bomb blasts and riots -- a lot of valuable information is available via online social media. However, all information obtained from OSNs are not trustworthy. Beside this, it is a challenge to extract important updates about an ongoing event (situational updates) from large volume of generic comments being posted. It is evident that utilizing OSNs during emergency situations involves several research challenges, some of which require further investigation than what has been done till now. There are additional challenges while dealing with disaster in third world countries like India where usage of OSNs is not so common, including scarcity of data, lack of updates by authoritative users, and so on. Hence, mechanisms to utilize OSNs during emergency situations in India need to be developed.

Kunal Banerjee
Email: kunalb@cse.iitkgp.ernet.in
Joined the department in: January 2010

Kunal Banerjee *received a B.Tech. degree in Computer Science & Engineering from Heritage Institute of Technology, Kolkata in 2008. Since January 2010, he has been a research scholar in the department of Computer Science & Engineering in IIT Kharagpur. Prior to his doctoral studies, he worked as an Assistant System Engineer in Tata Consultancy Services Ltd. His research interests are in the areas of Formal Verification and Embedded Systems.*

Supervisors: Prof. Chittaranjan Mandal and Prof. Dipankar Sarkar

Validation of Transformations of Embedded System Specifications using Equivalence Checking

In the last two decades extensive research has been conducted addressing the design methodology of embedded systems. Application areas of such systems include, but are not limited to, cars, telecommunication equipment, medical systems, consumer electronics, robotics, the authentication systems, etc. The source programs, in general, are subjected to significant optimizing transformations, automated and also human guided, before being mapped to an architecture. Due to the criticality of the services that these systems provide, it is of utmost importance to ensure that their behaviour do not get altered during the synthesis process. Translation validation was proposed as a new approach for the verification of compilers whereby, each individual translation is followed by a validation phase which verifies that the target code produced correctly implements the source code, rather than proving in advance that the code produced by the compiler is always correct by construction.

The objective of our work is to show the correctness of several behavioural transformations that occur during embedded system design using equivalence checking methods of the finite state machine with datapath (FSMD) model and its extensions. Following are the problem areas that we have worked upon and plan to pursue with deeper understanding in future.

1. Verification of Code Motions Across Loops: Code optimization is a common phenomenon during the scheduling phase of high-level synthesis to improve the synthesis results. The transformations reform the control structure of the code and often move code operations beyond basic block boundaries. Our research group has already proposed some solutions for this problem in their earlier works. Code motion transformations sometimes lead to code snippets being moved across loops, which our current method fails to handle. Literature survey reveals that almost no work exists to tackle code motions across loops. We have devised a (symbolic) value propagation based method that will be able to handle control structure modification as well as code motions across loops.

2. Verification of Array-Intensive Behaviours: To ensure correctness of loop and arithmetic transformations in array-intensive programs, array data dependence graphs (ADDGs) are employed. However, ADDGs suffer from the following shortcomings: single assignment form, no provision for specifying data-dependent index ranges and data-dependent control structures. So, we intend to enhance the FSMD model with arrays in order to overcome these deficiencies. The new model calls for categorization of the variables, a redefinition of the update function and the characteristic tuple of a path, and new normalization rules. The existing equivalence checking method for FSMDs exploits the similarity of the path structures of the two FSMDs to find equivalent paths. So, failure is encountered

for transformations, such as loop splitting and loop merging, that modify the control flow graph of a behaviour. Therefore, developing a methodology to attend to such transformations as well, while maintaining the current framework, seems to be a prospective future endeavour. Moreover, the mappings of the index spaces of the output arrays from those of the input arrays for the ADDGs corresponding to the original and the transformed behaviours are constructed in isolation before performing equivalence checking between them. In contrast, the equivalence checking of two FSMDs proceeds by identifying equivalent path segments in the original and the transformed behaviours revealing in the process the discrepancies, if any, between the respective mappings. Hence, it is anticipated that in case of non-equivalence, the procedure involving FSMDs will report it much earlier than that of ADDGs, pin-pointing the regions where they mismatch and therefore be of more help for debugging purposes. Furthermore, ADDGs being able to capture only the data flow graphs involving arrays have found application mainly in multi-media domain, whereas we aim at catering to a larger set of programs involving scalars and arrays that have undergone data as well as control flow transformations.

3. Deriving bisimulation relations through equivalence checking: Both bisimulation relation based method and path based equivalence checking approach are prevalent in the literature on translation validation of programs. The basic methodologies of these two approaches differ; the path based approach tries to obtain path covers in the two FSMDs such that each path in one is found to be equivalent with a path in the other and vice-versa, while the (conventional) bisimulation based approach tries to construct a relation that serves as a witness of the two programs being symbolically executed in an equivalent manner. Both these methods have their own merits and demerits. The bisimulation relation based approach can be used to validate complex transformations such as loop shifting which cannot be handled by the resent path based approaches. However, all methods that have adopted this approach fail to guarantee termination. These methods are, currently, highly susceptible to modifications of the control structure. On the other hand, the path based approach has been shown to be better equipped to handle control structure modifying transformations and this verification scheme is guaranteed to terminate. We aim to relate these two (apparently different) approaches by explaining how bisimulation relations can be derived from the outputs of the path based equivalence checkers. Developing a unified framework that encompasses all the benefits of these two approaches seems to be an interesting future work.

Manjira Sinha
Email: manjira@cse.iitkgp.ernet.in
Joined the department in: July 2009

Manjira Sinha *received a B.Tech. in Computer Science from Heritage Institute of Technology, Kolkata in 2009. Since July 2009, she has been a research scholar in the department of Computer Science & Engineering in IIT Kharagpur. Her research interests are in the areas of Natural Language Processing, Cognitive Science and Text Readability and Enhancement.*

Supervisor: Prof. Anupam Basu

Computational Modelling of Text Readability in Bangla: A Reader Oriented Approach

Text readability refers to all text properties that interact with a reader during reading and affect the extent of understanding of the text and the cognitive load. Readability or text difficulty depends on the lexical, syntactic, and semantic and discourse dimensions of the textual content along with the background of the reader and the concerned language. In spite of having many practical significances and huge user base, there are few attempts for text readability Bangla. In this thesis, I have studied text readability in Bangla in three textual levels: full text, sentence and word. A Bangla dataset in Unicode encoding has been prepared to make up for the unavailability of automatically accessible data in Bangla that is annotated according to the reading difficulty. User feedback has been recorded through a number of empirical user surveys using diverse methodologies. Two target user groups have been considered at every step of the work to study the subjective effect user background on text readability and to validate the final models. For full text readability, the research establishes the inapplicability of English readability formulae such as Flesch Reading Ease index for Bangla. Estimation models and binary classification models of Bangla text readability have been developed using regression analysis and support vector machines respectively. A short study has also been performed on the relation between the readability and latent semantic analysis in Bangla. In sentence level readability, I have studied both the effect of constituents and organization of words in a sentence on the comprehension difficulty. Regression method has been used at first to model user feedback on sentence reading difficulty with sentence attributes. In the next step, an entropy approach based on dependency grammar of Bangla has been used to model the user response with successive reading of words in a sentence. A computational model has been proposed based on depth of the dependency structure and number of unprocessed dependencies to measure processing difficulty of sentence surface forms. At word level, I have studied the effect of orthography through feature based complexity, phonology, semantics and word familiarity on written word recognition in Bangla.

Mayank Singh
Email: mayank4490@gmail.com
Joined the department in: December 2013

Mayank Singh *received his B.tech degree from IIT Jodhpur in May 2012. From August 2012 to May 2013 he worked in Infosys Limited. Since December 2013 he has been a research scholar in the department of Computer Science & Engineering in IIT Kharagpur. His areas of interest are in Machine Learning, NLP, Data Structures*

Supervisor: Prof. Pawan Goyal and Prof. Animesh Mukherjee

Scientific publications are means to communicate the results, ideas and innovation among the research community. These research documents are increasing with an annual rate of 2.5%. There are several metrics that are used over the years to measure the quality of these documents. Most of them are based on citations and H-index. Our idea is to use the Document content as a foundation and as support to get insight into document quality quantification. We would propose a metric based on a number of content features that will quantify scientific document quality and how the quality determines its impact. This impact could be measured at different levels: at the level of the document, or at the level of the venue where the document got published or at the level of individual scientists who published it.

Moumita Saha
Email: mousaha2012@gmail.com
Joined the department in: July 2012

Moumita Saha *received B.Tech. in Computer Science & Engineering in 2010 from WBUT and M.Tech. in Computer Science & Engineering in 2012 from Bengal Engineering & Science University. For her Ph.D. degree, she is working in the area of pattern recognition.*

Supervisor: Prof. Pabitra Mitra

Climate Data Mining for Indian Monsoon

Indian summer monsoon rainfall (ISMR) is a dynamic process, which considerably affects the economy of the country. It results from multiple sea-atmosphere interactions throughout the globe. Predicting ISMR is a challenging task due to presence of multiple influencing climatic parameters and involvement of complex mechanism.

Identification of climate indices influencing Indian monsoon and modelling Indian monsoon process is prime focus of the work. Different statistical and machine learning approaches are considered for discovery of novel climatic indices important for monsoon process and designing the forecast models. An attempt is made to study the variability of Indian monsoon over temporal window. A joint clustering approach of years and predictors is adopted to cluster the years according to different subsets of climatic parameters and homogeneity of patterns, thereby building the forecasting model with improved precision.

Climate index discovery assists in visualizing different aspects of climatic system. We focus on discovery of climate indices important for ISMR from climatic variables, namely, surface pressure, sea surface temperature, and wind velocity. Community detection approach is applied for the purpose. Discovered climate indices are found to be highly correlated to Indian monsoon process and they also ascertain their superiority in prediction of ISMR.

Deep Learning-based architecture is utilized to discover novel climate features that are relevant to Indian monsoon. It attempts to model high-level abstractions in data by using architectures composed of multiple non-linear transformations, where features are discovered and improvised at every layer. Finally, we aim to design a hybrid model by combining physics based global climate model and machine learning based model. Thereby, encashing the benefits of both models: (i) Physics based computational models move from knowledge (in the form of physical theories of climatic processes) towards data - a way of exploring how well current theory explains the data, and (ii) Machine learning based approach moves from data to knowledge - a mathematical model that describes the discovered relationships among the data.

Pankaj Kumar
Email : pankusoftech@gmail.com
Joined the department in: July 2014

Pankaj Kumar *received B.Tech degree in Computer Science And Engineering from Biju Patnaik University of Technology, Orissa in 2011. He received M. Tech degree in Software Engineering from National Institute of Technology, Durgapur in May, 2014. Since July 2014, he has been a research scholar in the Department of Computer Science & Engineering in Indian Institute of Technology, Kharagpur. His research interests are in Software Testing and Program Analysis.*

Supervisor: Prof. Rajib Mall

Effective Fault Localization

Often programs are large and complex. In typical software development project, maintenance is estimated to consume about 50% to 80% of the total development efforts. A major component of this is fault localization effort. Fault localization involves identifying the exact location of a program fault from the failure report. Once a failure has been indicated by execution of a test suite, zeroing down on the faulty statements has been acknowledged to be a non-trivial problem. Therefore effective automatic fault localization techniques that can guide programmers to locate the faults within program is an urgent practical necessity. An effective fault localization technique can achieve significant reductions to the bug search space and can lead to substantial reduction in debugging cost.

Several fault localization approaches for procedural programming languages such as "C", have been proposed in the literature. Broadly, the reported research can be categorized into control-flow based and dependency-based techniques. The dependency-based techniques show greater promise. However, all these research efforts have reported varying degrees of success in effectively localizing the faulty statement. The dependency-based techniques use a system dependency graph (SDG).

A major shortcoming of the reported work is that they do not scale well with the size of the program. On the other hand multimillion line programs have become common place. The reported work do not address how access to global variables, procedural calls, pointers and exceptions can be handled.

In this context, we propose a novel approach for effectively localizing faulty statements within the program. In our approach, we first construct system dependency graph for a given source program by determining control, data, and inter procedural dependencies from equivalent control flow graph of that program. We attach weights with the edges of the system dependency graph based on "suspiciousness" of a dependency contributing to the failure. The value of weights to the edges are determined by coverage information generated based on both the passed and failed test cases. We propose an approach, "Highest Weight Normalization (HWN)" to compute the weights for every exercised dependencies. Based on this we compute scores for nodes indicates their suspiciousness. This appears to be more realistic way to localize faults rather than considering a binary decision (faulty or non faulty) judgment on the individual statements as done in other approaches. We validated our approach using a number of open source programs available. We introduced faults into these programs and run the test cases to determine the pass and fail cases.

Further to address the scalability aspects, we plan to propose a dependency graph that has the functions as nodes, rather than having the statements as nodes. After having localized the fault to the functions, we plan to refine the localization to the basic block level and further to the basic statement level.

The novelties of our work is as follows:

1. We propose to use an established program model-SDG for fault localization. This enables to consider the dependencies that arise on account of access to global variables, procedural calls, pointers and exceptions. To the best of our knowledge no work is using SDG for fault localization has been reported.

2. We propose a novel weighted SDG where weights are associated with edges indicating the confidence that the edge propagate correct values. We propose a few weight assignment schemes based on the trace of passed and failed test cases.

Papia Mahato
Email: papiamahatostar@gmail.com
Joined the department in: December 2013

Papia Mahato *received a B.Tech. Degree in computer science and engineering from West Bengal University of Technology in 2008.From August 2008 to February 2009 she has done Diploma in Advanced Computing from C-DAC ACTS Pune. In year 2009 she joined Saba Software Inc. Ltd., Pune as Software Developer and left the organization in 2010 and joined Tech Mahindra .She left the company in 2011 for further studies. In year 2013 she passed M.Tech in computer science and engineering from Jadavpur University, Kolkata. Since December 2013, she has been a research scholar in the department of Computer Science & Engineering in IIT Kharagpur. Her research interests are in the areas of Digital Geometry.*

Supervisor: Prof. Partha Bhowmick

Parantapa Bhattacharya
Email: parantapa@cse.iitkgp.ernet.in, parantapa@gmail.com
Joined the department in: July 2010

Parantapa Bhattacharya *received his B.E. degree in Information Technology from Bengal Engineering and Science University, Shibpur in 2008, and his M.Tech. degree in Information Technology from IIT Kharagpur in 2010. Since July 2010, he has been a research scholar in the department of Computer Science & Engineering at IIT Kharagpur. His research interests are in the areas of Online Social Networks and Computer Security.*

Supervisors: Prof. Niloy Ganguly and Prof. Soumya Kanti Ghosh (SIT)

Topical Search in Twitter Online Social Network

Twitter is increasingly being used to search for information and current news on various topics. Recent studies [2, 4] have observed that the most common reasons for searching Twitter are obtaining information on trending topics and recent events. This motivates developing better services for topical search on the Twitter platform.

One of the primary requirements for implementing topical search, on an OSN is to discover topical attributes of the users who are the primary sources of information in an OSN [1, 5, 6]. To identify the topical attributes of Twitter users, we utilize social annotations of users (i.e., how other users describe a given user), which are collected by exploiting the Lists feature. Lists are an organizational feature, using which an user can group related Twitter accounts that is of interest to him/her, and view their collective tweet-stream. When creating a List, a user typically provides a List name and optionally adds a List description. The key observation is that many users carefully curate Lists to include important Twitter users related to a given topic, e.g. a List on music that includes Lady Gaga, Britney Spears, and so on. Furthermore, the creators of Lists generate meta-data, such as List names and descriptions, that provides valuable semantic cues to the topics of the users included in the List [3, 6].

We leverage our knowledge of topical experts to enable search for content on specific topics. We have designed a novel topical search system for Twitter, which, given a topic, identifies the tweets and trends (hashtags) being discussed by the community of experts on that topic. In brief, our system works as follows. We collect, in near real-time, the tweets being posted by the experts on a topic (as identified by the List-based methodology). We use a two-level clustering scheme to cluster the tweets that are related to the same news-story – we cluster the hashtags based on their co-occurrence in tweets, and cluster the tweets based on the hashtags they contain. Results (clusters of tweets and hashtags, which correspond to a news-story) are ranked by the number of distinct experts who have posted on the particular news-story. Based on a user-survey, we found that our methodology successfully mines tweets and hashtags relevant to a wide variety of topics. Additionally, since we rely on the content posted by a carefully identified set of topical experts, the results are trustworthy, i.e., free from spam.

References

[1] S. Dill, N. Eiron, D. Gibson, D. Gruhl, R. Guha, A. Jhingran, T. Kanungo, S. Rajagopalan, A. Tomkins, J. Tomlin, and J. Zien, “SemTag and Seeker: bootstrapping the semantic web via automated semantic annotation”, ACM World Wide Web Conference (WWW), 2003.

[2] G. Golovchinsky and M. Efron, “Making sense of Twitter search”, ACM CHI Workshop on Mi-croblogging: What and How Can We Learn From It?, 2010.

[3] N. Sharma, S. Ghosh, F. Benevenuto, N. Ganguly, and K. Gummadi, “Inferring Who-is-Who in the Twitter Social Network”, ACM Workshop on Online Social Networks (WOSN), 2012.

[4] J. Teevan, D. Ramage, and M. R. Morris, “#TwitterSearch: a comparison of microblog search and web search”, Web Search and Data Mining (WSDM), 2011.

[5] X. Wu, L. Zhang, and Y. Yu. “Exploring social annotations for the semantic web”, ACM World Wide Web Conference (WWW), 2006.

[6] P. Bhattacharya, S. Ghosh, J. Kulshrestha, M. Mondal, M. B. Zafar, N. Ganguly, and K. P. Gummadi “Deep Twitter Diving: Exploring Topical Groups in Microblogs at Scale”, ACM Computer Supported Cooperative Work and Social Computing (CSCW), 2014.

Priyanka Sinha
Email: mottee@gmail.com
Joined the department in: July 2012

Priyanka Sinha *has completed a BTech in Computer Science and Engineering from IIT Guwahati and MS in Electrical and Computer Engineering from Auburn University. She was awarded the Institute Merit Scholarship from 2000 to 2002 and Vodafone Fellowship from 2005-2006 for her outstanding academic records. She is currently a scientist at TCS Research. She is a TCS sponsored PhD candidate at IIT Kharagpur. Her current research interests are focused on Text Mining. She has also worked in the area of internet routing protocols and wireless networking at Ericsson.*

Supervisors: Prof. Pabitra Mitra and Prof. Anupam Basu

Mining group behavioral traits from enterprise text communications

Group behavior is how people interact with each other in a group. Groups can be small of 3 people and maybe large with thousands of people. A group in our context is not a mere aggregation but a collection of people who work towards a common cause. It is not essential that all members of a group work on the same task. A group executes multiple tasks in sub-groups all of which combine together to attain the common goal. Usually there is a higher-order task plan that is decided upon by the members of a group explicitly or implicitly. The task plan has tasks and objectives at multiple granularity which combines to align with the final goals and objectives. Consequently group structures are usually complex and may consist of several sub-groups, hierarchies and layers. Examples of groups that interest us are business enterprises who develop products or provide services, communities of people who work towards a common cause (common interest) like developing open source, social communities who work towards a common cause like women empowerment.

In recent times, several research groups have shown that it is possible to profile social media users along behavioral attributes based on their social-network behavior. Our proposition is that mining group communications can similarly yield information related to behavior attributes of members in a group and the role that these attributes play in group dynamics. We use enterprise social media text and emails to analyze group communications along the axes of content, persona and communication. Our results of mapping of employee word usage to established models of personality by psychologists have shown promise of further exploration.

R.Rajendra Prasath
Email: rajendra@cse.iitkgp.ernet.in
Joined in: 05 January 2009

R.Rajendra Prasath *received M.Sc [Mathematics] from Ramanujan Institute for Advanced Study in Mathematics, M.Tech [CSE] from Indian Institute of Technology, Kharagpur. During 2004-2006, he worked as an Assistant Professor in MNMJEC under Anna University, Chennai. Later Rajendra joined the CLIA Project as a Senior Project Officer. During August 2009 – September 2010, Rajendra worked at the Norwegian University of Science and Technology (NTNU), Norway as an ERCIM Alain Bensoussan Fellow. Rajendra was a Visiting Fellow at The Artificial Intelligence Research Institute (IIIA), Spanish National Research Council (CSIC), Barcelona, Spain and Swedish Institute of Computer Science (SICS), Kista, Sweden during May - June 2010. Earlier, Rajendra was a University Research Fellow at University of Madras, from November 2001 to April 2003. He also developed tools for Cross Lingual Information Access system [at IITKGP] as a part of DIT, Govt. of India sponsored research work. Presently Rajendra is a volumne editor of MIKE conference series. Rajendra served as a reviewer for journals: IEEE/ACM Transactions on Networking, Information Sciences, Journal of Convergence Information Technology and several popular international conferences. He is a professional member of ACM, International Rough Set Society (IRSS) – Warsaw and Information Retrieval Society of India. His research interests include cross language information retrieval, textual case based reasoning, machine learning, information retrieval and big data analytics for business intelligence.*

Supervisor: Prof. Sudeshna Sarkar

The Ordering of Contents in Information Retrieval

"Searching for Information" is ever growing activity of humans in their day to day life. Modern Information Retrieval (IR) systems attempt to understand the user information needs given in the form of a query composed of a set of keywords, perform the retrieval task on the specified collection of documents and output a ranked list of documents. User queries used to specify the information needs are often short having 2 - 3 keywords on average and often ambiguous. It is really challenging for IR systems to identify and fill the gaps in such queries. This reduces the effectiveness of the IR systems. Additionally, ranking of retrieved documents with more specific information to the user query becomes really challenging in IR systems. In this research work, we have considered the document retrieval problem with a special focus on the ranking / re-ranking of retrieved documents. Given a specific collection of documents, either web documents or ad hoc news documents, and an user information need, retrieve documents that are relevant to the user information needs in terms of various aspects like comprehensiveness, diverse aspects, domain specific aspects, and topic dynamics across multi-lingual news documents.

We have developed an approach to assist web documents retrieval using topic matching between query and documents [1]. We have identified the major types (topics) in the tourism domain and built an ontology of the tourism domain. We developed a document classifier to identify the topic of web documents, and a query classifier to identify the topic of the user query, both pertaining to the tourism domain. The proposed IR system performs document retrieval by matching the type of user query with the matching type of documents.

Then we have presented an approach to improve the ranking of the retrieved documents via query expansion using PRF-CBD algorithm [2, 6]. In this work, we have attempted to improve the ranking of the retrieved documents via query expansion using Pseudo Relevance Feedback based Clustering

By Directions (PRF-CBD) Approach that identifies additional terms for expanding the user query. These additional terms are then used to improve the effectiveness of documents retrieval.

We have developed an algorithm for ranking the comprehensive documents using segmentation and clustering of the document content [4]. The comprehensiveness of a web document may be estimated by analyzing various parts of its content, and checking diversity, coverage of the content and the relevance as well. The proposed approach ranks documents based on the comprehensiveness of the web documents as well as their relevance using pseudo relevance feedback.

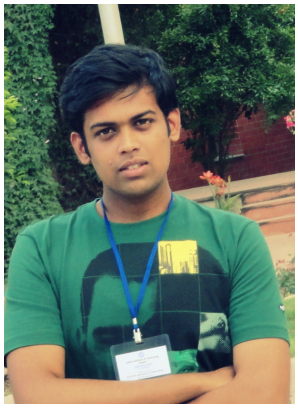
We have investigated the problem of capturing term contexts to identify semantically related information that could effectively disambiguate the user query and improve the retrieval efficiency of news documents [3]. This approach is based on random indexing, and identifies semantically related information that effectively disambiguate the user query. User query terms are expanded based on the terms with similar word senses that are discovered by implicitly considering the *associatedness* of the document context with that of the given query.

We present a cross language information retrieval approach to effectively retrieve information present in a language other than the language of the user query using the corpus driven query suggestion approach [2]. The idea is to utilize the corpus based evidence of one language to improve the retrieval and re-ranking of news documents in another language. We used FIRE dataset with Tamil and English news collections and illustrated the effectiveness of the proposed CLIR approach.

Rajib Lochan Jana
Email: jlrajib.cse@gmail.com
Joined the department in: January 2014

Rajib Lochan Jana *received his B. Tech. degree in Computer Science and Engineering from Government College of Engineering & Textile Technology, Berhampore, India and M.Tech in Information Security from Motilal Nehru National Institute of Technology Allahabad, India. He has worked as assistant professor at ICFAI University, Tripura. Mr. Jana is currently working toward the PhD degree at Computer Science & Engineering department, IIT Kharagpur, India. His current research interests include Theory of Computation, Formal Verification Methods and Embedded System Design.*

Supervisors: Prof. Soumyajit Dey and Prof. Pallab Dasgupta



Rajorshee Raha
Email: rajorshee.raha@cse.iitkgp.ernet.in, rajorshee87@gmail.com
Joined the department in: July 2013

Rajorshee Raha *did his B.Tech. and M.Tech. in Electronics and Communication Engineering from WBUT in 2009 and 2011, respectively. For his PhD work, he is working on validation of embedded real-time control.*

Supervisors: Prof. Pallab Dasgupta and Prof. Partha Pratim Chakrabarti

Validation of Embedded Real Time Control

An Embedded System is a specialized computer system that is part of a larger computer or machine. A Real-Time System is a type of system in which the performance of the system not only dependent on their logical correctness but also on the time at which the results or outcomes are produced. A Control system is a system that manages, commands, directs or regulates the behavior of other device or systems. Hence, a Real-Time Embedded Control System can be quoted as a system, which is an integrated part of a larger system and controlling the system behavior, performance with some timing constraints [1, 5]. It has a vast area of application in many Industries such as Automotive control, Home appliances, Telecommunication systems, Automated manufacturing systems, medical equipments, Defense and military applications, etc. Examples of embedded systems are Mobile Phones, Modern Car safety systems like Anti-lock braking system (ABS) Controller, Adaptive Cruse Control system(ACC) etc.

Multi-mode Sampling Period Selection for Embedded Real Time Control: In Embedded Real Time Control systems, the computational resources are generally limited and must be used as efficiently as possible. At the same time demand for integrating more and more functionality to the system is also increasing. Thus several concurrent tasks need to be executed using the limited available resources. Hence, it is preferable to have efficient methods that optimize the performance of control loops in the system with scare computing resources [2]. Embedded software-based control systems have traditionally been implemented by assuming fixed sampling rates and fixed task periods[6]. Adaptive regulation of the sampling rate may theoretically determine the optimal balance between computational efficiency and control performance [4, 3] but such schemes are difficult to implement in practice due to non-determinism in timing introduced by the computational infrastructure (including message delays, execution time variations in different paths of the control software, etc).

So we are currently working on proposing a Mode Based Scheduling of Embedded Control System, where scheduling will be different in every mode of execution. The mode selection is done using control theoretic analysis and also based on certain scenarios the controller is going to work. Sampling rates in each of these modes will vary depending upon the above analysis measures. Further we are working on to provide a supervisory automata which will supervise the mode switching as well as the scheduling. Formally establishing a verification methodology the properties of this Mode Based Scheduling scheme is also a prospective area of our future research.

References

[1] K. Astrom and B. Wittenmark. Computer controlled systems: theory and design. Prentice-Hall information and system sciences series. Prentice-Hall, 1984.

[2] G. Buttazzo. Research trends in real-time computing for embedded systems. SIGBED Rev., 3(3):1–10, July 2006.

[3] A. Cervin, M. Velasco, P. Marti, and A. Camacho. Optimal online sampling period assignment: Theory and experiments. Control Systems Technology, IEEE Transactions on, 19(4):902–910, 2011.

[4] D. Henriksson and A. Cervin. Optimal on-line sampling period assignment for real-time control tasks based on plant state information. In Decision and Control, 2005 and 2005 European Control Conference. CDC-ECC ’05. 44th IEEE Conference on, pages 4469–4474, 2005.

[5] Q. Li and C. Yao. Real-Time Concepts for Embedded Systems. CMP books. Taylor & Francis, 2003.

[6] D. Seto, J. Lehoczky, L. Sha, and K. Shin. On task schedulability in real-time control systems. In Real-Time Systems Symposium, 1996., 17th IEEE, pages 13–21, 1996.

Ranita Biswas
Email: biswas.ranita@gmail.com
Joined the department in: July 2012

Ranita Biswas *did her B.Tech. in Information Technology from Kalyani Government Engineering College, West Bengal, in 2009. From July 2009 till July 2010, she worked as a Project Linked Personnel in Indian Statistical Institute, Kolkata. In 2012, she received her M.E. degree in Computer Science and Engineering from Bengal Engineering and Science University, Shibpur, and then joined the PhD programme in the Department of Computer Science and Engineering at IIT Kharagpur. Her research interests are in the areas of Digital Geometry, Computer Graphics, and Mathematical Imaging.*

Supervisor: Prof. Partha Bhowmick

Digital Spheres and Geodesics: Characterizations, Algorithms, Applications

Our research is centered on theoretical properties of discrete spheres and geodesics in the domain of *digital geometry*, which is an upcoming specialization of *discrete geometry* in the integer space. Combinatorial properties of configurations of discrete objects (points, lines, planes, circles, spheres, etc.) in the integer space are investigated in the field of digital geometry. It offers sophisticated analysis and techniques with practical efficiency to a mathematician or a computer scientist while working with digitized models or images of objects in 2D or 3D space. Unlike real geometry, digital geometry does exact computation in the problem space with guaranteed approximation error, since a *digital object* essentially consists of a set of elements (points, manifolds, etc.) that are specified by integer coordinates.

We have so far worked on topologically well-defined models of 3D digital spheres using elementary number-theoretic and graph-theoretic techniques. We have designed an efficient integer algorithm to generate a 3D digital sphere for a given integer radius and integer center. The algorithm is based on number-theoretic properties of digital sphere and marked by simple integer operations, easy implementation, efficiency, and exactness. We have further shown how these number-theoretic properties can be tuned to *rapid prototyping* of a digital sphere for 3D printing through layer-by-layer additive fabrication. We have also designed an efficient integer algorithm for finding *discrete geodesic paths* on spherical surfaces. This algorithm is based on certain topological and number-theoretic characterization, and runs in optimal time.

Currently, we are working on creation of *graceful spheres* for generation of smoother geodesics and *Mobius polygons* on spherical surfaces. Our forthcoming work includes identification of *persistent patterns* in a digital sphere and generation of *iso-contours* on digitized 3D surfaces.

Sandipan Sikdar
Email: sikdarsandipan99@gmail.com
Joined the department in: December 2012

Sandipan Sikdar *received his B.tech degree in computer science and engineering in July, 2012 from Institute of Engineering and Management, kolkata. Since December 2012, he has been a research scholar in the department of Computer science and engineering at Indian Institute of Technology, Kharagpur. His research interests are in temporal and dynamic networks.*

Supervisors: Prof. Animesh Mukherjee and Prof. Niloy Ganguly

Unsupervised metrics to compare community detection and clustering algorithms

In the Big Data era, efficient means to extract information from large datasets have acquired a particular relevance. Researchers from varied fields are increasingly turning on to big data analytics for investigating the underlying mechanisms of any complex system. From understanding gene regulation and genome evolution to modeling various intricacies of human behavior, big data analytics is finding application everywhere. Nevertheless, it ultimately relies on the ability to identify relevant variables, distinguishing them from uninteresting details, which may be considered as noise. This leads us to a very interesting and active area of research which is called dimensionality reduction. Here we focus on the problem of partitioning given a list of objects (or data points) the problem is that of dividing them into groups of similar ones. While in the computer science literature this problem is popularly known as clustering, in the physics literature this problem corresponds to community detection in networks. In both the fields, numerous algorithms have been proposed for data clustering and community detection. These rely on different measures of similarity between the data points. However, there is no consensus on which algorithm to choose for a specific partitioning task. The central problem is that there is no universal criterion for selecting a particular method and the holy grail of the “perfect algorithm” likely does not exist. In cases where comparison with a ground-truth classification is possible, different algorithms are found to perform better in different cases The key idea is to measure two different entropy values (i) H[S] which is the entropy of the size distribution of the clusters obtained and (ii) H[K] which is the weighted entropy of the size distribution of the clusters where weights denote the frequency of a particular size cluster. The main focus of the work is to show that these measurements allows one to derive an unsupervised measure to rank different partitioning methods. More precisely, for a given resolution H[S] we claim that the algorithm that achieves a classification with a higher value of H[K] should be preferred. Besides this local (resolution dependent) criterion, we also propose a global criterion to rank algorithms at all resolutions. The global criterion is based on the area under the H[S] − H[K] curve generated by varying the parameter responsible for producing different cluster size distributions for a particular method. We believe that our method tries to replicate the actual underlying process of community formation rather than trying to measure the goodness of the outcome unlike all other validation metrics Note that these measurements can be easily extended to the analysis of time-varying networks and we plan to conduct the same as an immediate following objective.

Sanjoy Pratihar
Email: sanjoy.pratihar@gmail.com
Joined the department in: July 2011

Sanjoy Pratihar *received his B.Tech in Computer Science and Engineering from North Eastern Hill University, Shilong, India, and received his M.E. in Computer Science and Engineering from Bengal Engineering and Science University, Shibpur, India. Currently he is a PhD scholar in the Department of Computer Science and Engineering, Indian Institute of Technology, Kharagpur, India. His research interests include digital geometry, document image processing, graphics analysis, and intelligent human-computer interaction. He has served as a lecturer in the Department of Computer Science and Engineering, University Institute of Technology, The University of Burdwan, Burdwan, India.*

Supervisor: Prof. Partha Bhowmick

On Some Digital-geometric Applications of Farey Sequence

Background: In the year 1816, John Farey invented an amazing procedure to generate proper fractions lying in the interval [0,1], called the *Farey sequence* [5,6]. It remained unattended and unexplored for almost a century until the beginning of last century. And in recent times, with the emergence of various algorithms in the digital/discrete space, several interesting works have come up related with the Farey sequence.

Our Idea of Augmented Farey Table: The Farey sequence of order *n* is the sequence of simple/irreducible, proper, positive fractions with denominators up to *n*, arranged in increasing order (Fig. 1). The concept is well-known in *theory of fractions*, but from the algorithmic point of view, very limited work has been done so far. In our work, we have augmented a Farey sequence with compound fractions, improper fractions, and negative fractions, which do not find any place in the original sequence. With all these *fraction ranks*, we build the *Augmented Farey Table (AFT).* We have used the AFT for several interesting applications, as mentioned below.

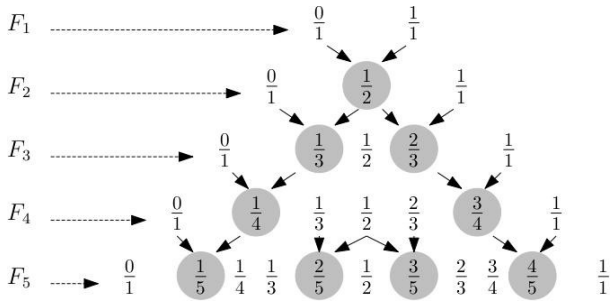
Polygonal approximation: An efficient boundary representation of an object in the digital plane is done through polygonal approximation. During approximation, “reasonably collinear” straight edges are successively merged. The collinearity is tested by edge slope, which corresponds to AFT rank. If the *rank difference* of two edges is less than a prescribed tolerance, then the two edges are merged into a single edge in an iterative manner. With the idea of *exponential averaging*, the AFT has been used by us for polygonal approximation in gray-scale images without any edge detection and thinning [1].

Shape Representation: If all the internal angles are written in order for a polygon, we get an idea about its shape. As a novel alternative, we have used the sequence of rank differences corresponding to adjacent edges. This has subsequently been used for shape decomposition [2], shape matching [4], etc.

Vectorization of Thick Digital Lines: Vectorization of a digital object provides a succinct, space-efficient, and useful representation for several applications in computer graphics and image analysis. As a fast and efficient vectorization of digitized engineering drawings, we have used AFT for geometric analysis and refinement [3].

Correction of skew: An algorithm for detection and correction of skews present in scanned document images is proposed using analysis of ranks of fractions in a Farey sequence. Straight edges are derived and binned by their Farey ranks, which, in turn, are analyzed to obtain the principal bin from the sums of lengths of the edges in a sequence of bins. The principal bin corresponds to the principal direction, from which the skew angle is estimated to finally correct the skew.

Conclusion: Usage of AFT enables all our algorithms to be devoid of floating-point operations, thus saving a significant amount of runtime. The notion of AFT also puts forward some important theoretical issues, such as compressing an AFT, as its size is quadratic with the order of Farey sequence.



		Denominator								
		-4	-3	-2	-1	0	1	2	3	4
N	4	19	18	16	14	13	12	10	8	7
u	3	20	19	17	15	13	11	9	7	6
m	2	22	21	19	16	13	10	7	5	4
e	1	24	23	22	19	13	7	4	3	2
r	0	25	25	25	25	–	1	1	1	1
a	-1	26	27	28	31	37	43	46	47	48
t	-2	28	29	31	34	37	40	43	45	46
o	-3	30	31	33	35	37	39	41	43	44
r	-4	31	32	34	36	37	38	40	42	43

Figure 1. Left: Farey sequences of orders 1 to 5. Right: AFT of order 4.

References

[1] S. Pratihar and P. Bhowmick, A thinning-free algorithm for straight edge detection in a gray-scale image. In Proc. 7th Intl. Conf. on Advances in Pattern Recognition (ICAPR), pages 341–344. IEEE CS Press, 2009.

[2] S. Pratihar and P. Bhowmick, Shape decomposition using farey sequence and saddle points. In Proc. ICVGIP-2010, pages 77–84. ACM, 2010.

[3] S. Pratihar and P. Bhowmick, Vectorization of thick digital lines using Farey sequence and geometric refinement. In Proc. ICVGIP-2010, pages 518–525. ACM, 2010.

[4] S. Pratihar and P. Bhowmick, "On applying the Farey sequence for shape representation in Z^2", Book Chapter, Speech, Image and Language Processing for Human Computer Interaction-Multi-modal Advancements , Chapter 9, pp. 172–190, U. S. Tiwary and T. J. Siddiqui (Ed.), IGI Global, 2012.

[5] D. Knuth R. Graham and O. Potashnik, In Concrete Mathematics. Addison-Wesley, 1994.

[6] M. Schroeder. Fractions: Continued, Egyptian and Farey (chapter 5), number theory in sc. and communication. Springer Series in Information Sciences, vol.7, 2006.

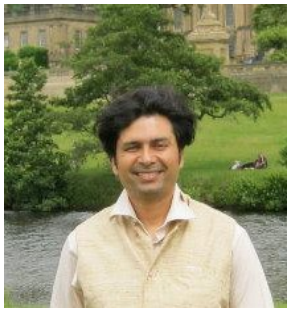
Sarani Bhattacharya
Email: sarani.bhattacharya@cse.iitkgp.ernet.in, tinni1989@gmail.com
Joined the department in: July 2013

Sarani Bhattacharya *received her B.Tech. in Computer Science and Engg. from St. Thomas College of Engineering and Technology, Kolkata in 2011 and M.Tech. in Computer Science and Engg. from Indian Institute of Technology, Kharagpur in 2013. Since July 2013, she has been a research scholar in the department of Computer Science & Engineering in Indian Institute of Technology Kharagpur. Her research interests are in the areas of Cryptography and side channel analysis on microarchitectural events such as branch misses, prefetching.*

Supervisor: Prof. Debdeep Mukhopadhyay

Impact of Micro-architecture on Side-channel Attacks

With the ever-increasing proliferation of e-business practices, great volumes of secure business transactions and data transmission are routinely carried out in an encrypted form in devices ranging in scale from personal smart cards to business servers. These algorithms are often computationally intensive and most implementations of these algorithms leak information through side-channels such as power, timing, and electro-magnetic radiation of the device. These side-channels can be exploited by an adversary to gain information about the secret encryption key. Preventing these side-channel attacks is difficult because the leakage not only depends on the cipher algorithm but also on the implementation and its execution platform. Further, several of these leakages stem from vulnerabilities in the underlying hardware. For example, attacks on systems have been demonstrated using inherent vulnerabilities present in architectural components such as cache-memories, branch-prediction units, hyper-threading units, etc. These attacks were called micro-architectural attacks. Countermeasures proposed for micro-architectural attacks so far are generally ad-hoc and applied at the application layer. There are several drawbacks of countering side-channel attacks in the application layer. First, most of the countermeasures are heavy and inefficient. Further, all applications sharing the same host require to apply these countermeasures to protect against a common vulnerability. This adversely affects performance and energy requirements of the system. Second, a countermeasure to prevent one attack may lead to new attack techniques, which use the same vulnerabilities. The alternative is to develop CPUs that are inherently secure against side-channel attacks. That is, the CPU architecture is designed with innate abilities to contain information leakage. To build such systems requires the identification and quantification of information leakage due to variouscomponents in the micro-architecture, and then the development of new micro-architectural components that considers security as a per-requisite along with other design parameters such as performance and power consumption. The effect of the conflict misses, scheduling algorithms, performance counters which are implemented for the processors can be exploited to show that they leak information. The analysis can be actually helpful in designing secure systems that inherently prevent these leakages.



Saranya Saha
Email: saranya_saha@hotmail.com
Joined the department in : July 2014

Saranya Saha *received a B.E. degree in Computer Science and Engineering from Jadavpur University, Kolkata, India in 1997, a M.S. degree in Computer Science from University of Massachusetts, Amherst, MA, USA in 1999 and a M.A. degree in Linguistics from University of Pennsylvania, PA, USA in 2002. Since July, 2014, he has been a Research Scholar in Computer Science and Engineering Department at IIT Kharagpur. His research interests include Natural Language Processing, Historical Indo-Aryan (Vedic, Sanskrit, Prakrit, etc.) and the Indian approach to languages. He has joined the MHRD funded SANDHI project in the language group.*

Supervisor: Prof. Pawan Goyal and Prof. Sudeshna Sarkar

Saurav Kumar Ghosh
Email: saurav.kumar.ghosh@gmail.com
Joined the department in: December 2013

Saurav Kumar Ghosh *received a B. Tech degree in Computer Science & Engineering from Kalyani Government Engineering College in 2013. Since December 2013, he has been a research scholar in the department of Computer Science & Engineering in Indian Institute of Technology Kharagpur*

Supervisor: Prof. Soumyajit Dey

Early Analysis of System Reliability using Probabilistic Program Models

The reliability of a system is increasingly being considered as a first class criteria in the design space of mission critical as well as soft real-time systems. However, automated synthesis and verification tool flows for such reliable embedded systems are still in their infancy. Another drawback of such works would be that the granularity of the analysis is (un)fairly coarse grained.

Existing techniques for component based software reliability analysis constructs a task graph based representation of modular software systems. The estimates thus derived do not take the following points into consideration.

• The probability distribution of the possible inputs.
• The execution semantics of the program.
• The failure probability of the underlying hardware of a hardware software co-designed system.
• The absence of an initial model for functional reliability analysis.

Probabilistic programs can serve as initial models for functional modeling of reliable systems and formal analysis methods can be used for validating such models, leveraging model checkers and theorem provers for counter example based refinement of probabilistic programs. A subsequent step is integrating such analyses into synthesis tools for embedded system design.

To this end, we propose RELSPEC, a framework for early reliability analysis and refinement of embedded applications with support for explicit reliability constructs. The behavioral description of a system can be captured via RELSPEC, for reliability analysis at an early stage of its design flow. RELSPEC can also provide reliability refinement if the system does not meet its desired reliability.

Sayan Mandal
Email: mesayaan@gmail.com
Joined the department in: July 2014

Sayan Mandal *received a B.Tech. degree in Computer Science and Technology from West Bengal University of Technology, Salt Lake in 2012, and an M.E. degree in Computer Science and Engineering from Indian Institute Institute Engineering Science and Technology, Shibpur in 2014. He is the recipient of the Prof. A.K.Seal Gold Medal from IIEST Shibpur, for securing first position at the master's level in the university. Since July 2014, he has been a research scholar in the Department of Computer Science & Engineering in IIT Kharagpur. His research interests are in the areas of Image processing and computer vision.*

Supervisor: Prof. Jayanta Mukhopadhyay and Prof. Prof. Partha Pratim Das

Segmentation of Tumour cells from colo-rectal region and radiation treatment planning

The studies on medical image processing has gained momentum for over two decades when scientists from the fields of computer science, electronics and electrical started collaborating with doctors and medical representatives to provide better tools for treatment and analysis of patients. The state of the art equipment that are used today range from machineries for disease diagnosis like MRI, PET and ultrasonography etc. to the transplantation of artificial hearts; to the use of automated bots for successful surgery. With respect to the treatment of cancer, the very basis lies on the detection and localisation of cancerous cells in different parts of the human body. These tumour cells are then treated with process of radiation where ionizing electromagnetic waves are injected targeted to the malignant cells so as to burn them.

The project investigates the possibilities of automatic localisation of tumour cells in the colon and rectal regions of human body. At present, the delineation of these cells are done manually by a medical practitioner given a PET or CBCT image. The problem that persists is offcourse the time taken by doctors to segment cancer cells from each slide of images, the process being tedious and erroneous. An automated technique would give a real time accurate segmentation of such tumour cells. Further, due to the present day inaccuracies of delineation, the radiation therapy is performed on a rectangular window around the tumour cells. Thus many healthy cells are destroyed each time a patient is treated with radiation. The objective of the project is to investigate if tumour cells can be identified with the highest degree of accuracy such that only those voxels of the tomography representing the cancer affected cells are localised. Till date several techniques have been tested for the segmentation of various organs and tissues of the human body. Some tissues can be directly segmented based on a Hounsfield scale which measures the relative inability of electromagnetic radiation to pass through the particular tissues. Other segmentation methods are on the basis of 1) statistics and probability [2], 2) graph theory [1] and 3) image processing and soft computing [3]. The reason why none of these techniques are able to extract the cancer cells in colon regions in because of its non-rigid nature. The colon has no fixed location and changes shape frequently due to the presence of fluids or gas which makes it all the more difficult to identify.

Besides the objective of segmenting the colorectal cancer cells, many other aspects need to be analysed. One such requirement is to find a mathematical relation between the shifts of the bone contour with the volume of the colon. This finding will enable oncologists to draw a direct relation between the skeletal and colorectal regions of human body. The other investigation is to find the effects of the dosage and duration of radiation on the progressive change of tumour cells. There is not always the case that a radiation therapy leads to the reduction of cancer cells, as sometimes, the tumour may even undergo a growth post a radiation. A relational mapping of this change in tumour volume with the dosage and frequency of radiation would help doctors in future treatment planning.

Reference

[1] Survey on liver CT image segmentation methods, Artif Intell Rev, Springer(2012)

[2] Partial Volume Tissue Classification of Multichannel Magnetic Resonance Images-A Mixel Model, IEEE TRANSACTIONS ON MEDICAL IMAGING, 1991[3] An adaptive fuzzy C-means algorithm for image segmentation in the presence of intensity inhomogen

Shyantani Maiti
Email: shyantani.maiti@cse.iitkgp.ernet.in
Joined the department in: December 2013

Shyantani Maiti *is a PhD scholar in the Department of Computer Science and Engineering in Indian Institute of Technology, Kharagpur since December 2013. She has received M.E degree in Computer Science and Engineering from Indian Institute of Engineering Science and Technology, Shibpur (former Bengal Engineering and Science and University) in 2011. She has received a B.Tech degree in Computer Science and Engineering from M.C.K.V. Institute of Engineering, West Bengal University of Technology in 2006. Her research interests are in the area of bioinformatics and computational biology.*

Supervisor: Prof. Pralay Mitra

Understanding the mechanism of membrane proteins on bacterial motility

Living organisms including bacteria move for several reasons. One of the major reasons is the movement in search of food that is directly related with the survival of the bacteria. Chemotaxis is the movement of an organism in response to a chemical stimulus. Single-cell or multicellular organisms direct their movements in response to certain chemicals present in their environment. This is important for organisms such as bacteria to find food (e.g., glucose) by swimming toward the highest concentration of food molecules. In short, performing the chemotactic movement helps an organism to drive itself toward the gradient of a particular chemical (especially food). Flagella present in bacteria helps it to move toward or away from the chemical stimulus. Because of the availability of the vast amount of literature we will focus on *Escherichia Coli (E. coli)* to study the flagellar movement helping in chemotaxis. The bacterial chemotaxis has only two states: (i) Counter-clockwise rotation (CCW), where flagella forms a single rotating bundle, causing the bacteria to swim in a straight line; (ii) Clockwise rotation (CW), where flagella bundle breaks apart such that each flagellum points in a different direction, causing the bacterium to tumble in place.

The chemotaxis signaling system of *Escherichia coli* modulates the function of the cell's flagella motors. *E. coli* cells migrate toward favorable glucose environments in response to extracellular signals by controlling the rotational direction of flagella motors from anticlockwise to clockwise. Chemoreceptors (sensory receptor that transduces a chemical signal into an action potential) modulate the phosphorylation (post translational modification of proteins on which serine, threonine, or a tyrosine residue is phosphorylated by a protein kinase by the addition of covalently bonded phosphate group) activity of a histidine protein kinase, CheA, and the phosphoryl group on CheA is rapidly transferred to a response regulator, CheY. Phosphorylated CheY(CheY-P) functions as an activated intracellular signaling molecule. Phosphorylated CheY which binds to FliM subunits in the motor, is believed to induce a switch in rotation from a counter clockwise (CCW) to a clockwise (CW) direction.

Our research amis to develop an algorithm and perform extensive computation to detect the structure and binding of several flagellar proteins. It will also help us to identify the mechanism of chemotactic movement of bacteria.

Soumadip Biswas
Email: soumadip.cse@gmail.com
Joined the department in: July 2014

Soumadip Biswas *received a M. Tech degree in Information Technology from Indian Institute of Technology, Kharagpur in 2012, an B. Tech degree in Compute Science & Engineering from West Bengal University of Technology in 2010. From July '2012 till May '2014, he worked in Citrix R&D (India) Pvt. Ltd. as Software Engineer. Since July 2014, he has been a research scholar in the department of Computer Science & Engineering in Indian Institute of Technology, Kharagpur. His research interests are in the areas of Computer Networks, specifically Software Defined Networking.*

Supervisor: Prof. Arobinda Gupta

Soumajit Pramanik
Email: soumajit.pramanik@gmail.com
Joined the department in: July 2013

Soumajit Pramanik *received his B.Tech. degree in Computer Science & Engineering from St. Thomas' College of Engineering & Technology, Kolkata in 2011 and his M.Tech degree in Computer Science from Indian Statistical Institute, Kolkata in 2013. Since July 2013, he has been a research scholar in the department of Computer Science & Engineering in IIT Kharagpur. His research interests are in the areas of interdependent networks, information-flow dynamics, data mining & machine learning.*

Supervisor: Prof. Bivas Mitra

In my research, I mainly focus on analyzing information propagation in different types of networks. Two types of information flows which have drawn most of the attentions of the researchers, are i) knowledge information flow and ii) social information flow. In every type of information propagation, there exist some dormant hidden factors which can play crucial roles in deciding the properties (like size, speed etc.) of the diffusion. In this work, we want to analyze both types of information flows to identify those dormant factors and propose new models for information diffusion dynamics keeping them in consideration.

i) Knowledge information flow:
In real-life, knowledge propagation (flow of ideas) in scientific domain is specifically indicated by citations and collaborations. In this context, we study whether social interactions between researchers in the scientific conferences can eventually get converted into mutual citations and develop new collaborations. For the benefit of the scientific community, we also propose a "Recommendation System" which recommends an author about the persons with whom she may try to interact during her up-coming conference, for increasing her citations and building new collaborations.

ii) Social Information Flow:
In case information propagation in OSNs (example: Twitter, Facebook etc.), there is a specific role of mediators/information-brokers (e.g. “Mention” in Twitter) who help to spread the information beyond the immediate reach of social neighbours. So, here we try to understand how this mediators (e.g. “Mention” in Twitter) facilitates any information flow in an OSN (e.g. Twitter). We model the information flow dynamics utilizing the framework of multiplex networks and propose a "Recommendation System" to recommend a user about the persons she can mention in her tweet, to make it more popular in a shorter time.

Soumyadip Bandyopadhyay
Email: soumyadip@cse.iitkgp.ernet.in
Joined the department in: January 2009

Soumyadip Bandyopadhyay *received a B.Tech degree in Computer Science & Engineering from Bengal Institute of Technology, Kolkata in 2008. Since January 2009, he has been a research scholar in the department of Computer Science & Engineering in IIT Kharagpur. His research interests are in the areas of Formal Verification and Embedded Systems.*

Supervisors: Prof. Chittaranjan Mandal and Prof. Dipankar Sarkar

Validation of Behavioural Transformations during Embedded System Synthesis using PRES+ Models

We focus on some aspects related to modeling and formal verification of embedded systems. Many models have been proposed to represent embedded systems [2]. These models encompass a broad range of styles, characteristics, and application domains and include the extensions of finite state machines, data flow graphs, communication processes and Petri nets. Here, we have used a PRES + model (Petri net based Representation for Embedded Systems)[1] as an extension of classical Petri net model that captures computation, concurrency and timing behaviour of embedded systems; it allows systems to be represented in different levels of abstraction and improves expressiveness by allowing the token to carry information. This modeling formalism has awell-defined semantics so that it supports a precise representation of a system.

A typical synthesis flow of complex systems like VLSI circuits or embedded systems comprises several phases. Each phase transforms/refines the input behavioural specification (of the systems to be designed) with a view to optimizing time and physical resources. Behavioural verification involves demonstrating the equivalence between the input behaviour and the final design which is the output of the last phase. In computational terms, it is required to show that all the computations represented by the input behavioural description, and exactly those, are captured by the output
description. The input beaviour undergoes several transformation steps before being mapped to an architecture. Our objective is to verify those transformation steps.

Specifically, we address two issues namely, (1) automated checking of functional equivalence of the transformed optimized behavioural specification to the original one, also referred to in the literature as transformation validation and (2) comparison of timing performances of the behaviours of the design before and after the optimizations are applied. While the sequential behaviour can be captured by FSMDs, the parallel behaviour can be easily captured using PRES+. An equivalence checker for FSMD models already exists [3].

Hence, we have formulated an algorithm to translate a PRES + model into an FSMD model and use the existing FSMD equivalence checker. It is to be noted that the timing constraints are inconsequential for demonstrating data transformation equivalence between the behaviours which allows us to perform equivalence checking using FSMDs. However, translation of a PRES+ model into the corresponding FSMD model encounters state explosion because the method essentially

involves parallel composition of the concurrent transitions in PRES+. Moreover, the state explosion problem is further aggravated due to various possible interleavings of the concurrent transitions, which may come into play when timing analysis is addressed. Therefore, we have formulated a direct equivalence checking between two PRES+ models. In this direct equivalence checking method we have captured the computation of a PRES+ model at some out-port as the concatenation of parallel paths. Then using the path equivalence between the original and transformed PRES+ models, we have devised the equivalence checking calculus. In this equivalence checking method, there are

some sophistications needed, such as path extension. However, unlike strictly sequential control flow of FSMDs, PRES+ models capture the concurrent control flow more vividly; exploring this feature the overhead of path extension has been avoided using a modified path decomposition of the PRES+ model.

A future work will be a comparative study of the three equivalence checking methods, one via translation from PRES+ models to FSMDs and checking equivalence of the translated FSMDs and the two methods checking equivalence of PRES + models directly. Specifically, we intend to address code motion validation for this comparative study.

Next we aim at enhancing the PRES+ equivalence checker for time optimizing transformations and also loop transformations.

References:

[1] L. A. Cort´es, P. Eles, and Z. Peng. Verification of embedded systems using a petri net based representation. In ISSS ’00: Proceedings of the 13th international symposium on System synthesis, pages 149–155, Washington, DC, USA, 2000. IEEE Computer Society.

[2] S. Edwards, L. Lavagno, E. A. Lee, and A. Sangiovanni-Vincentelli. Design of embedded systems: Formal models, validation, and synthesis. In Proceedings of the IEEE, pages 366– 390, 1997.

[3] C. Karfa, D. Sarkar, C. Mandal, and C. Reade. Hand-in-hand verification of high-level synthesis. In GLSVLSI ’07: Proceedings of the 17th ACM Great Lakes symposium on VLSI, pages 429–434, New York, NY, USA, 2007. ACM.

Sourav Kumar Dandapat
Email: sourav.dandapat@gmail.com
Joined the department in: July 2009

***Sourav Kumar Dandapat** is* pursuing his PhD from Computer Science and Engineering dapartment,IIT Kharagper under the supervision of Prof. Niloy Ganguly. I am also a member of Complex Network Research Group (CNeRG) and working in a project titled "Enhancing Cloud Efficiency Through P2P based Architectures" funded by CSIR. Before joining IIT Kharagpur, I worked at Magma Design Automation India Pvt. Ltd, Bangalore, India for one year three months as Associate Member of Technical Staff and before that I worked at IBM ISL for two years and five months as System Software Engineer. I received M. Tech in Computer Science and Engineering from Indian Institute of Technology Kharagpur in 2005 and B.E. degree from Jadavpur University in Computer Science and Engineering in 2002.

Supervisor: Prof. Niloy Ganguly

Some Techniques to Address Traffic Congestion and Capacity Constraints in Mobile Networks

As a result of the popularity of mobile devices, mobile data traffic is increasing in exponential rate. According to the Cisco's prediction this trend will continue and by end of 2018 mobile data usage will be around 16 Exabyte per month compared to the 1:5 Exabyte in 2013. To manage this enormous mobile data traffic one single step is not adequate. We have identified three issues related to mobile data traffic management as our objective of this thesis - (1) Eefficient offload using Wi-Fi Network, (2) Managing Heterogeneous Traffic and (3) Restricting Unauthorized Traffic.

Efficient offload using Wi-Fi Network: Cellular networks are becoming heavily congested and to ooffload this traffic, Wi-Fi network becomes a promising solution. However, it is still difficult for a Wi-Fi network to support a user with high mobility, especially for applications with high-bandwidth requirement like video streaming. In this work, we propose to host popular les in local memory that can be attached with Wi-Fi AP. This solution, reduces access delay and increases throughput significantly. Main challenge of this project is to design spatial distribution scheme to distribute le chunks across APs to utilize limited memory attached with AP in efficient way.

Managing Heterogeneous Traffic: From different study of human mobility model, it is known that trac across network (spatially) is not evenly distributed. Simple association strategies result in overloading some access points while most of the access points remain under utilized. To overcome this issue, we create a global view of load distribution through out of band communication among APs and also reduce association control problem to classical Max-Flow problem. Our proposed association control protocol can handle the uneven load distribution and accommodate maximum clients.

Restricting Unauthorized Traffic: There are many paid services which grant access to valuable content like movies, news, songs etc. People used to share their subscription credential of such services either under social pressure or to reduce per head subscription charge. As an effect this increases unauthorized traffic. To restrict sharing of credential, we propose a new dynamic authentication scheme based on user's daily activity. For evaluation purpose, we develop a system which considers

browsing history, Facebook activities, and phone activities. Our system collects users' activities, select potential activities for challenge generation, get response from users and verify responses to authenticate.

Sourya Bhattacharyya
Email: sourya.bhatta@gmail.com
Joined the department in: July 2012

Sourya Bhattacharyya *received B.E. degree from Jadavpur University, Kolkata in 2006, and obtained M.S. degree from Indian Institute of Technology Kharagpur in 2012. From July 2012, he is pursuing PhD in the field of Computational Modeling of Evolutionary Genomics. Currently, his research focuses on the development of algorithms modeling the phylogenetic evolution, using input DNA or protein sequences.*

Supervisor: Prof. Jayanta Mukhopadhyay

Algorithms for constructing evolutionary trees

Phylogenetic trees represent evolutionary relationships between 'taxa' (entities such as genes, populations, species, etc.). Every leaf of the tree uniquely represents one taxon. For individual species (taxa), its representative such as a gene (DNA) or protein sequence are used as inputs. Analyzing the similarity among those representative biomolecular sequences is the first part of phylogenetic tree construction. Higher similarity (or lower distance) among a pair of taxa (actually their representative sequences) indicate that they should be very closely related. In the phylogenetic tree representation, the taxa pair is shown to be evolved from a common ancestor (represented as an internal or non-leaf node) close to the leaves. On the other hand, highly distant taxa pairs are represented by having their common ancestor close to the root itself. Pairwise distances among a group of N taxa are stored in a *distance matrix* of dimension N × N, which is subsequently used for phylogeny reconstruction.

For a large set of taxa (N is of the order of thousands), estimating pairwise distances among all the taxa pairs is often not possible, due to absence of common representative biomolecular sequence across all the taxa. One solution is to build small scale phylogenetic trees for taxa subsets having common representative biomolecular sequences. The taxa subsets themselves need to be overlapping (complete or partial), and their union should cover the input taxa set. In such a situation, we can synthesize those input trees to form a *Supertree* depicting the evolutionary relationships among complete taxa set. However, input phylogenetic trees may associate conflicts (different evolutionary relationships among a set of taxa) among themselves, due to the fact that individual trees may be constructed from different biomolecular sequences (having different characteristics and evolutionary changes) and also by different phylogeny construction methods. Resolving such conflicts to produce the supertrees depicting preferably the consensus (most frequent) evolutionary relationships among individual taxa subsets, is an NP-hard problem.
If individual phylogenetic trees cover same taxa set, but are constructed by sampling different gene sequences representing those taxa, the trees are termed as *gene trees*. For multi-locus genome analysis, individual gene trees may associate conflicts or variations in the evolutionary relationships among taxa subsets. The objective is to derive a *species tree*, depicting the evolutionary relationships among the taxa set, which matches the input tree topologies as closely as possible. Such species tree can be constructed either by concatenating input gene tree sequences followed by sequence based phylogeny estimation, or employing a supertree or consensus analysis on input gene tree topologies. Major difference between such species tree estimation and standard supertree estimation technique lies in the fact that species trees may depict non-consensus (less frequent) evolutionary relationships among individual taxa subsets, thus not conforming to the input gene tree topologies.

Our research constitutes above mentioned two problems. First, we have developed a supertree construction algorithm using couplet (taxa pair) relationships, having cubic and quadratic time and space complexities, respectively, which are lower or equal to the existing studies. The algorithm is proved to be highly accurate, in terms of the topological similarities between the derived tree and input phylogenetic trees. We are currently focusing on adapting the supertree algorithm to produce species trees from a set of incongruent gene trees. The objective is to develop an approximation which can lower the incongruence among input gene tree topologies with the derived species tree.

References:

1. J. Felsenstein, *Inferring phylogenies*. Sinauer Associates, 2003.
2. B. R. Baum. *Combining trees as a way of combining data sets for phylogenetic inference, and the desirability of combining gene trees.* Taxon, 41:3-10, 1992.
3. M. S. Swenson, R. Suri, C. R. Linder, and T. Warnow, *Superfine: Fast and accurate supertree estimation,* Syst Biol, vol. 61, pp. 1-14, 2011.
4. James H. Degnan and Noah A. Rosenberg. *Gene tree discordance, phylogenetic inference and the multispecies coalescent.* Trends in Ecology and Evolution, 24(6):332-340, 2009.

Sreejith M
Email: sreejm@gmail.com
Joint Department in: January 2015

Sreejith. M *received his M.Tech degree from National Institute of technology Rourkela in Electronics Systems and Communication Engineering, in June 2014. He received his B.Tech degree from university of Calicut in Electronics and Communication in June 2007. From December 2007 to October 2008, he worked as a software engineer in UST-BLOBAL. From October 2008 to January 2012 he worked as programmer analyst at General Electric Hyderabad. His research interests are in Robotics, Computer vision and embedded vision.*
His broad area of research will be robotics.

Supervisors : Prof. Dr. Partha Pratim Das and Prof. Dr. Katja Mombaur of Universität Heidelberg

Subhasish Dhal
Email: sdhal@cse.iitkgp.ernet.in, subhasis.rahul@gmail.com
Joined the department in: December 2009

Subhasish Dhal *received a B. Sc(H) degree in Computer Science from Vidyasagar University, Midnapore in 2002, and a MCA degree from NIT Durgapur in 2005. He also has received an M. tech degree in Computer Sc. And Engineering from NIT Rourkela in 2009. From August 2005 till August 2007 he worked in Asutosh College, Kolkata as a lecturer (contractual) and from August 2009 till December 2009 he worked in IE & IT, Durgapur as a lecturer. Since December 2009, he has been a research scholar in the department of Computer Science & Engineering in IIT Kharagpur. His research interests are in the areas of Security in RFID and Mobile Networks.*

Supervisor: Prof. Indranil Sengupta

Object Identification in RFID Technology

An object needs to be identified for various reasons. Radio Frequency Identification (RFID) technology helps to identify it efficiently. However, the existing solutions in this technology have many security implications. Location privacy is one of such problems and this thesis proposes a solution to fix this problem in the existing protocols. The detection probability can be increased by attaching multiple number of RFID tags to the object. However, the existing protocols do not have such assumption. The focus of this thesis is to increase the security of the object by utilizing multiple number of tags. Authentication is a necessary task to verify the legitimacy of information communicated through an insecure medium. However, appropriate authentication scheme in multi-tag environment is absent in the literature. This thesis proposes two secure authentication protocols in multi-tag environment. Searching an object from a large set is another problem which cannot be solved using any authentication scheme. A secure protocol for object searching problem in multi-tag environment has also been proposed in this thesis. Many applications require a proof of coexistence of a set of relevant objects to avoid any wrong execution. A secure proof generation protocol in multi-tag environment has been proposed as the final contribution in this thesis. The proposed protocols in this thesis are lightweight and this is one of the key requirements in RFID technology.

Subhrangsu Mandal
Email: santu.cst@gmail.com
Joined the department in: January 2014

Subhrangsu Mandal *received a B.E.. degree in Computer Science and Technology from Bengal Engineering and Science University, Shibpur in 2009. From July 2009 to July 2010, he worked as an Associate System Engineer in IBM India Pvt. Ltd. After that he received M. Tech. degree in Computer Science and Engineering from IIT, Guwahati in 2012. From July 2012 to January 2014, he worked as a Software Engineer 2 in Citrix R&D India. Since January 2014 he has been a research scholar in the department of Computer Science and Engineering. His research interests are in the areas of Distributed Systems.*

Supervisor: Prof. Arobinda Gupta

In last few decades the advent of various mobile computing devices like smart phone, laptops etc. has introduced networks where the network topology changes very frequently. The appearance and disappearance of nodes and edges are very common in those networks. There are also other types of networks, such as vehicular networks where nodes move very fast, distortion tolerant network where nodes and communication links can disappear at any time because of extreme conditions etc., which exhibit very frequent change in topology. Research in these areas has shown that the traditional static graph model is not enough to model and analyze these systems. So the concept of dynamic graph where edge and node set changes very frequently, has been introduced by researchers.

Construction and maintenance of certain graph structures like spanning tree, connected dominating set, independent set etc. are important problems in the area of distributed computing. As an example, a spanning tree provides an efficient communication path between all nodes in a network, which can also be used to collect different network-wide information such as total number of nodes present in the network, maximum id of any node in the network etc. These information are very useful to solve other fundamental problems such as leader election, information dissemination, termination detection etc. Hence efficient algorithms to construct and maintain spanning trees on dynamic graphs can be used as basic building block to solve many fundamental distributed computing problems on dynamic graphs. Note that the problem is more challenging in dynamic graphs as in many cases the structure itself is not defined clearly. For example, the definition of a spanning tree in static graph does not carry over directly to a dynamic graph as the dynamicity may imply that any spanning tree may not exist at a single time step, though a spanning tree may be established by taking union of the graphs over several time steps. There are many other example of such graph structures such as dominating sets and connected dominating sets, independent sets etc. Building and maintenance of graph structures in distributed environment has been well-explored for static networks but has hardly been dealt with in the context of dynamic networks. Hence, construction and maintenance of graph structures on dynamic graph is the focus of my research.

Sudakshina Datta
Email: sudakshina.dutta@gmail.com
Joined the department in: July 2011

Sudakshina Datta *received B.E. degree in Information Technology from Jadavpur University in 2007. From July 2007 to June 2009, she worked as Member of Technical Staff in Interra Systems India Pvt. Limited. She joined Department of Computer Science and Engineering of Indian Institute of Technology Kharagpur and received M.Tech degree in July, 2011. Since then, she has been a research scholar in this department and her research interest includes Formal Verification of Concurrent Systems.*

Supervisor: Prof. Dipankar Sarkar

The parallelizing compilers has become very relevant in the prevalent high performance computing systems. To get significant speedup for a specific parallel architecture, suitable parallel programs have to be written. These compilers are used to automatically parallelize sequential program which is easier to write for an user.

The parallelizing compilers apply parallelizing transformations such as, loop concurrentization and loop vectorization to sequential programs. They transform a sequential source program to its parallel version with the same functionality. Moreover, various scheduling techniques such as, trace scheduling, percolation scheduling exist which enhance the process of parallelization. These techniques optimize usage of resources in the process of parallelization and produce an even more effective set of parallelizing transformations. Often parallelizing compilers apply various enabling transformations such as, induction variable elimination, scalar expansion, etc., at the earlier stages to eliminate data dependences that hinder the application of the parallelizing transformations. The enabling transformations cover some loop transformations such as, loop interchange,loop-fission,loop-fusion,etc.

With the commencement of the new era of massively parallel computers, there is a growing need to verify the correctness of the parallelizing compilers. To the best of our knowledge, none of the available literature has given a complete procedure for validation of the parallelizing process of existing parallelizing or vectorizing compilers. We have enhanced the methods of equivalence checking method for array handling programs for validating parallelizing transformations.

Suman Kalyan Maity
Email: sumankalyan.maity@cse.iitkgp.ernet.in
Joined the department in: July 2011

Suman Kalyan Maity has received his B.Tech. degree in Computer Science & Engineering from National Institute of Technology, Durgapur in 2011. Since July 2011, he has been a joint MS-PhD research scholar in the department of Computer Science & Engineering at IIT Kharagpur. His research interests are in the areas of complex systems, language dynamics and social networks.

Supervisor: Prof. Animesh Mukherjee

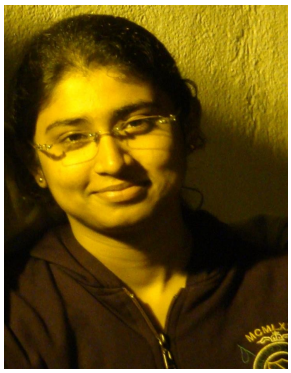
#Bieber + #Blast = #BieberBlast: Early prediction of popular hashtag compounds

Hashtag is the new “paralanguage” of Twitter. What started as a way for people to connect with others and to organize similar tweets together, propagate ideas, promote specific people or topics has now grown into a language of its own. As hashtags are created by people on their own, any new event or topic can be referred to by a variety of hashtags. This linguistic innovation in the form of hashtags in a very special feature of Twitter which has become immensely popular and are also widely adopted in various other social media like Facebook, Google+ etc. and have been studied extensively by researchers to analyze the competition dynamics, the adoption rate and popularity scores. However, there are very few attempts to study the linguistic aspects of hashtag evolution over large time scales. One of the interesting and prevalent linguistic phenomena in today's world of brief expressions, chats etc. is hashtag compounding where new hashtags are formed through combination of two or more hashtags together with the form of the individual hashtags remaining intact. For example, #PeoplesChoice and #Awards together form #PeoplesChoiceAwards. #MTVSports and #JustinBieber make #MTVSportsJustinBieber; #OregonBelieveMovieMeetup is formed by #Oregon, #BelieveMovie and #Meetup; #Educational, #Ipad, #Apps together form #EducationalIpadApps etc.

In etymology, we come across a very similar phenomenon where words are formed from various other words sampled from the same or a different language. Lexical compounding has been prevalent all through over the history of evolution of any language. For example, in English, 'wheelchair' has been formed from 'wheel' and 'chair', bookworm is the combination of 'book' and 'worm' with meaning of the words getting completely modified due to compounding. Similarly, 'in so far' has become 'insofar' with no meaning getting altered. However, such compounding phenomena in social media are far more prevalent than in standard texts and language. Further, hashtag compoundings happen at very short timescales compared to years/centuries in case of languages.

Innovation and adoption are both important processes in language change. While innovation refers to the creation of new linguistic units, adoption refers to its proliferation among wider groups of speakers. An innovative form must be adopted by a significant number of speakers in order for observable change to take place. We study the hashtag compounding phenomena as a linguistic innovation. In particular, we investigate, in detail, the socio-linguistic reasons for such compounding through a precise quantitative approach. This thorough investigation finally converges into a prediction model that can identify with 76.47% accuracy if a pair of hashtags compounding in the near

future shall become popular. This technique has strong implications to trending hashtag recommendation since newly formed hashtag compounds can be recommended early, even before the compounding has taken place. Experiments with human subjects show that humans can predict compounds with an overall accuracy of 48.7% (treated as baseline) thus indicating that it is an extremely non-trivial task to identify suitable features that govern the phenomena of compounding. We successfully identify a series of such features which allows us to achieve an overall accuracy improvement of 57% over the baseline.



Sumana Ghosh
Email: sumanaghosh@cse.iitkgp.ernet.in, sumana61189@gmail.com
Joined the department in: December 2012

Sumana Ghosh *received a B.Sc.(Hons) degree in Computer Science from University of Calcutta, Kolkata in 2010, and an M.Sc degree in Computer & Information Science from University of Calcutta, Kolkata in 2012. Since December 2012, she has been a research scholar in the department of Computer Science & Engineering in IIT Kharagpur. Her research interests are in the areas of formal verification.*

Supervisor: Prof. Pallab Dasgupta

Formal Specification and Verification of Reliability in Real Time Embedded System

In every sphere of our daily life, from automobiles to elevators, water heaters to cell phones, we increasingly depend upon embedded systems and expect them to operate as designed. Now-a-days, many embedded applications have become “safety-critical”, such as electronic braking systems, temperature monitors in water heaters, and most control components in the domains of aviation, automotive, railway signaling, atomic energy, space technology and industrial automation. Such embedded systems need extraordinary care during the design phase to not only ensure that they are safe at the time of commissioning, but also that they remain reliable over a designated period of time.

Intuitively, reliability is the probability that a system functions correctly over a period of time under given operating conditions. The term “functional correctness” encompasses a wide range of requirements, ranging from the correctness of the control algorithm, correctness of the software code, meeting power and timing constraints, and reliability constraints. Many of these attributes are related to each other. For example, the timing of sensing and actuation of control has a direct impact on stability and control performance. In the case of real-time embedded control systems, typically the real-time aspect is captured by the period and deadline of software components, which together specify the required frequency of execution of the control tasks. To guarantee reliability, system engineers must further introduce redundancy in the schedule of execution of various control tasks.

While reliability and fault tolerance have been widely studied, both for individual and component based systems, the need for capturing reliability at the specification level is being felt with increasing design complexity. The trade-off between cost and safety is well established in industrial practice, and in many sectors components having the same functionality but varying in terms of cost and reliability are prevalent. The modern embedded system designer is not only aware of these choices, but must also analyze the impact of these choices on the overall reliability and fault tolerance of the system to be designed. Ms Ghosh's aim is to formally capture this relation and develop formal methods to support/analyze reliability trade-offs at an early stage of the design flow.

Another important consideration towards designing reliable embedded systems is in understanding the prognosis (health monitoring) of the system as a function of degradation of the components over time. The embedded system designer must be able to leverage statistical knowledge about the degradation of components over time while designing a system that is guaranteed to remain reliable over a specified period of time. Her intention is to enable the formal specification of such requirements and validate

them over the designed system.

Component based systems often degrade gracefully when the control adaptively compensates the failure of one or more components using a mutated control strategy over the healthy components. Therefore, in modern cyber-physical systems, failures of individual sub-systems do not necessarily lead to a catastrophic failure of the entire system. This is undoubtedly a beneficial aspect of such systems, but it is also the case that for such systems, the task of analyzing whether the system is approaching a catastrophic failure is very complex and often not well understood. A classic example of such a system is the smart electrical grid, where the definition of health in itself is a matter of considerable research.

Her research intends to explore techniques for formal specification and validation of reliability and fault tolerance in large scale cyber-physical systems with the view that such methods will introduce a semantic rigor into the definition of health for such systems and lead to platforms for intelligent decision making based on formal models of predicted failures and the specified fault tolerance methods.

Sumanta Pyne
Email: sumantapyne@gmail.com
Joined the department in: December 2009

Sumanta Pyne *is a research scholar in the Department of Computer Science and Engineering at Indian Institute of Technology, Kharagpur, since January 2010. He is pursuing Ph.D. under the guidance of Professor Ajit Pal. His current area of research is Power Aware Software. His research interests include Software Techniques for Energy Efficient Computation, Low Power issues of Multicore Processors, Computer Architecture, Compilers, and Network Mobility. Prior to joining IIT Kharagpur, Sumanta received the degree of Master of Engineering in Computer Science and Engineering in 2009 from Bengal Engineering and Science University, Shibpur (formerly Bengal Engineering College, Shibpur and presently Indian Institute of Engineering Science and Technology, Shibpur). In 2005, he graduated from Meghnad Saha Institute of Technology on receiving the degree of Bachelor of Technology in Computer Science and Engineering, awarded by West Bengal University of Technology. He did his schooling at Birla High School (formerly Hindi High School). He started his professional career as a programmer at Hi-Q Solutions, Kolkata and then worked as a lecturer at Techno India College of Technology, Kolkata.*

Supervisor: Prof. Ajit Pal

Power Aware Software

The objective of the research work done for the thesis titled “Power Aware Software” is to introduce new compilation techniques for reducing dynamic, switching and leakage power on modern processors. The works “Power Aware Software Prefetching” and “Energy Efficient Multiway Branch Translation Techniques” saves dynamic power dissipation. The work “Loop Unrolling with Partial Gray Code Sequence for Array Computations” minimizes energy consumption bus switching activity. The work “Loop Unrolling with Fine Grained Power Gating” saves runtime leakage power of unused functional units. The work “Energy Optimization Techniques for OpenMP” does joint optimization of dynamic and leakage power saving for parallel programs using OpenMP which run on multicore processors. Each of the work is discussed in details in the following sections.

1. *Power Aware Software Prefetching*
Software prefetching is a performance oriented optimization technique, which is generally used to reduce the gap between processor speed and memory access speed. When software prefetching is applied to memory intensive benchmark programs, the performance improves with higher power consumption. The present work provides a mechanism to transform a program with software prefetching to its power aware equivalent. This is done by executing the software prefetching program at different voltagefrequency pairs. Besides reducing the power, the performance has been improved by adjusting the prefetch distance. XEEMU-Panalyzer simulator is used to evaluate the present work. Experimental results of the proposed scheme guarantees that performance improvement of software prefetching program is possible at the cost of less power consumption. The proposed work can enable a compiler to generate power aware software prefetching program.

2. *Energy Efficient Multiway Branch Translation Techniques*
Branch Target Buffer (BTB) plays an important role for pipelined processors in branch prediction during the execution of loops, if then else, call return, and multiway branch statements. It has been observed that 20% of instructions in a program are related to branch. Access to BTB consumes 10% of total energy consumption of a program in execution. This work introduces the use of kd-tree and pattern matcher to generate efficient code, i.e. lesser execution time, for multiway branch. However,

instead of enhancing performance, Voltage Frequency Scaling (VFS) can be applied to achieve energy efficiency without degradation in performance. The present work is evaluated on a wide range benchmark programs. The BTB energy saving in this present work lies in the range 20% to 80% with small improvement performance as well. The total energy reduction is in the range 312%.

3. *Loop Unrolling with Partial Gray Code Sequence*
This work introduces the translation of a loop with array computation to its loop unrolled version with partial Gray code sequence. This software technique reduces switching activity as well as energy consumption on the address bus of on chip data memory, which is independent of process technology parameters. Loop unrolling with partial Gray code sequence is suitable for array computations where there are sequential access of array elements, which allows to reschedule the access of array elements in a Gray coded sequence of their addresses, in each iteration of the unrolled loop. The expressions for switching activity and energy consumed on the address bus of the onchip data memory are derived for both unrolled loop with and without partial Gray code sequence. The proposed translation method finds a relocatable base address of the array so that the partial Gray code sequence is maintained, without any energy performance overhead and achieves a considerable amount of energy reduction without any performance loss. Array unification is introduced for multiple arrays taking part in computation within a loop. An algorithm that performs array unification and translation of the loop with multiple arrays to its loop unrolled version with partial Gray code sequence, has been proposed. The efficacy of the proposed approach is evaluated on five sample programs and ten benchmark programs. 10–93% reduction in switching activity and 10–94% reduction in energy dissipated on the address bus of on chip data memory have been achieved.

4. *Loop Unrolling with Fine Grained Power Gating*
This work introduces a compilation technique to reduce runtime leakage power of functional units of a processor by combining loop unrolling with power gating. The instructions in the unrolled loop are scheduled to provide opportunities for power gating the functional units which are not used for a considerable amount of time. Two algorithms, one without considering performance loss due to execution of power gating instructions and the other with maximum leakage energy savings without performance loss due to execution of power gating instructions have been introduced. These algorithms do loop unrolling, scheduling of instructions and finally insert power gating instructions. The present work is explained using two illustrative examples, one without loop carried dependence and the other with loop carried dependence. It is observed that the number of clock cycles taken by the power gating instructions is less than or equal to the number of clock cycles saved by loop unrolling. This results in 23–64% reduction of the total energy consumed by the benchmark programs without any degradation of performance.

5. *Energy Optimization Techniques for OpenMP*
This work introduces energy efficient scheduling of OpenMP parallel loop on multicore processors having finegrained dynamic voltage frequency scaling (DVFS) and dynamic threshold voltage scaling (DVTS) facility. Slack iterations in an OpenMP loop schedule are partitioned among the cores to obtain an energy efficient loop schedule. The slack iteration partitioned among the cores allow to apply DVFS and DVTS, to reduce dynamic and leakage energy consumption. Considering the time taken by the original OpenMP loop schedule as deadline, the clock frequency and supply voltage of the cores are scaled down, and the threshold voltage of the cores are scaled up. A constant time loop scheduling algorithm has been proposed, which guarantees a loop schedule consuming minimum energy for a given OpenMP loop schedule. The energy efficient loop schedules are obtained for static, dynamic, guided and runtime OpenMP loop scheduling algorithms. The energy efficient versions of work sharing and critical section constructs in OpenMP are also introduced. The combination of DVFS and DVTS causes substantial reduction in dynamic and leakage energy with negligible delay and energy overhead. The proposed approach is tested on four sample programs and ten benchmark programs, which achieves 5-35% reduction in energy.

Surjya Ghosh
Email: surjya.ghosh@gmail.com
Joined the department in: January 2015

Surjya Ghosh *is currently a PhD student in the department of Computer Science and Engineering at IIT Kharagpur. He has done his B.Tech degree in Computer Science and Engineering from Haldia Institute of Technology in 2003. He completed M.Tech in Information and Communication Technology from School of Information Technology at IIT Kharagpur in 2014. He has around 11 years of professional experience. He has mainly worked in area of SAP CRM in these years for various organizations (TCS, IBM and Capgemini).*

Supervisor: Dr. Bivas Mitra, Prof. Niloy Ganguly

I am working in the area of Mobile Affective Computing. Currently, I'm focussing on to identify emotional state of the user based on the smartphone application usage. For this purpose we are collecting data from the smartphone and trying to classify the emotional state of the user by applying some machine learning techniques.

Tanmoy Chakraborty
Email: its_tanmoy@cse.iitkgp.ernet.in, its_tanmoy@yahoo.co.in
Joined the department in: December 2011

Tanmoy Chakraborty *received B.Tech degree in Computer Science and Engineering from Kalyani Government Engineering College, Kalyani, Nadia (affiliated to West Bengal University of Technology, Kolkata), in 2009 and M.E degree in Computer Science and Engineering from Jadavpur University, Kolkata in 2011. Since December 2011, he is a research scholar in the Department of Computer Science & Engineering, IIT Kharagpur. He has been awarded with Google India Ph.D. fellowship in July, 2012. His research interests are in the areas of Complex Networking, Social Networking, Graph Theory and Natural Language Processing.*

Supervisors: Prof. Animesh Mukherjee and Prof. Niloy Ganguly

Community Identification in Large Scale Networks

Many complex systems tend to be hierarchically organized with certain entities interacting more often among each other than with the rest of the entities in the system. Detecting communities of such entities is of great importance in sociology, biology and computer science disciplines where systems are often represented as a network of entities. This problem is very hard and not yet satisfactorily solved, despite the huge effort of a large interdisciplinary community of scientists working on it over the past few years. The ability to find and analyze such groups can provide us with a solid understanding of fairly independent compartments in the network each of which possibly tend to play a special role that significantly affects the overall functional behavior of the system. In addition, such decompositions also allow for a better visualization of the structural characteristics of the system. The problem becomes even harder because of no prior knowledge of the underlying gold standard community structure of a network which otherwise could be employed to evaluate the accuracy of the detection method. So the detection as well as the evaluation of the ‘goodness’ of community structure of a network are both challenging.

Though the traditional approaches in community detection have been refined using new metrics, new research challenges arise due to the intrinsic dynamicity of nodes and links. Some of them include detection of overlapping communities (nodes with equal involvement in two or more communities), constant communities (recurrent groups of nodes that constantly remain together under any circumstances), mobility of nodes across communities in a time varying environment and investigation of the reasons for the cohesiveness of the in-group members. Therefore we are planning to make our mainstream researches under these fundamental ingredients of the community formations in large scale complex networks.

Beyond the theoretical work which has a general appeal, we are targeting a specific network – the citation network to answer several questions using community analysis. For example, studying the large scale citation networks and finding its community structure can reveal the clustering of different subjects of interest and its inter-dependencies. We have investigated the dynamics of scientific research communities in Computer Science domain and revealed several interesting observations. For instance, we have seen a symmetric pattern of climbing and declining trends among the top impactful research fields of computer sciences over the last fifty years. We have systematically tried to unfold the probable reasons behind the transitions of research directions. Furthermore, the problem has

formed an interesting shape when we introduced the effect of continental researches over the universal trend of research directions. We have concluded that global research is controlled majorly by the researches of North American scientists. We are trying to build a recommendation system that could predict the future research trend based on the previous results.

Such large scale citation networks could sometime serve as the origin of few other networks like collaboration networks, field-field networks, field-author bipartite networks etc. We have started working with collaboration network with the following question in mind: can the intrinsic trust among the pair of collaborators be one of the stepping stones to produce future collaborations? Do we recommend a ranked list of possible collaborators of a given author? The preliminary results strongly emphasize our intuition mentioned above. We are following this motivation to build a collaboration recommendation system from the co-authorship network.

We have pointed out several such problems on the direction of the community formation and its applications in large scale complex networks. We would also like to stress upon the scalability of community detection algorithm and reconfigure them on the platform of parallel programming such that they could suitably approximate the community detection output on the large size complex networks with small amount of complexity involved.

Tanwi Mallick
Email: tanwi.mallick@cse.iitkgp.ernet.in, tanwireachesu@gmail.com
Joined the department in: December 2011

Tanwi Mallick *is a TCS Research Scholar. She received her B.Tech and M.Tech in Computer Science from Jalpaiguri Govt. Engineering College (2008) and NIT, Durgapur (2010) respectively. From July 2010 to December 2011, she taught at DIATM College, West Bengal as an Assistant Professor. Tanwi joined the Department in December 2011 as an Institute Research Scholar and received the TCS Fellowship in October 2012. Her research interests are in the area of Computer Vision.*

Supervisors: Prof. Partha Pratim Das and Prof. Arun Kumar Majumdar

Characterization of Kinect Depth Data to Improve Image Capture for 3D Reconstruction

Indian Classical Dance (ICD), an ancient heritage of India, consists of visual (posture, movements, and expressions), auditory (music, tempo, rhythm, and intonation) and textual (lyric of the song) information that tell a story through body movements, hand gestures, vocal and instrumental music, facial expression (emotion), costume, and make-up. With time, these dance forms have been interpreted and performed by different artists in different ways and various sets of complex rules have emerged for body postures and gestures.

In my research work I intend to automate the analysis and interpretation of different forms of ICD and extensively use Bharatanatyam for my explorations. Specifically, I work on classification of Adavus (elementary movements in making a Bharatanatyam dance) based on recognition of body movements, hand gestures and emotions, detection of tabla beats and synchronization of music with movements, on transcription and interpretation of ICD. I use Kinects here to analyse and interpret the multimedia aspects of ICD.

Automated analysis and interpretation of dance can be useful in several ways. It can help (1) Create dance tutoring systems, (2) Preserve cultural heritage by dance transcription, (3) Synthesize and create animated avatars, (4) Interpret ICD in the context of society and culture, and so on.

Tapas Kumar Mishra
Email: tap1cse@gmail.com
Joined the department in: July 2013

Tapas Kumar Mishra *received a B.Tech. Degree in Computer Science & Engineering from Veer Surendra Sai University of Technology, Burla in 2010. He received a M. Tech. Degree in Computer Science & Engineering from Indian Insitute of Technology Kharagpur in 2013. Since July 2013, he has been a research scholar in the department of Computer Science & Engineering at IIT Kharagpur. His research interests are Combinatorics, Graph and Hypergraph Theory, Computational Geometry, and Ramsey Theory.*

Supervisor: Prof. Sudebkumar Prasant Pal

Bicoloring Cover for *k*-Uniform Hypergraphs

Suppose that there are n doctors, each can be assigned one of two kind of tasks; either he can see the patients or he performs the laboratory work. Each doctor is equivalent and he cannot perform both the tasks simultaneously. There are m groups of doctor, namely $S_1, S_2, ..., S_m$, each of size k. Each group are assigned to treat patients of particular community. A doctor can be a member of multiple groups, hence he can treat patients of different communities. Now in order to provide proper treatment to any community, every member of any k-sized group should not be assigned the same work (bad event). Now given n doctors and m communities, is there a possible assignment of tasks to doctors such that every community gets the proper treatment, given the doctors can work in multiple shifts? What is the minimum number of shifts the doctors need to make to cover all the communities?

This problem can be mapped to a set of bicolorings of a k-uniform hypergraph $G(V, S)$, $|V| = n$, $|S| = m$, with the doctors representing the vertices, the groups being the k-uniform hyperedges, the task assigned to the doctors is a bicoloring of vertices, with the bad events of hyperedge becoming monochromatic. The minimum number of shifts required for the doctors is the minimum size of the set of bicolorings, i.e. bicoloring cover number $\chi^c(G)$. We define Bicoloring Cover number χ^c as the minimum number of bicolorings required such that every hyperedge is properly bicolored(i.e non monochromatic) in some bicoloring. Formally: let $G(V, S)$ be a hypergraph with vertex set V , $|V| = n$, and hyperedge set S. X be a set of bicolorings $\{X_1, X_2, ..., X_n\}$. Then X is a bicoloring cover for G if $\forall e \in S$, $\exists X_i$ such that e is non-monochromatic with X_i . The minimum cardinality of all such X's is called Bicoloring Cover number $\chi^c(G)$.

Our current line of research focuses on determining the relation of number of hyperedges $|E|$ and dependency of any hyperedge d with $\chi^c(G)$. Initially we check the maximum number of hyperedges and maximum dependency for which $\chi^c(G) = 2$ is satisfied and then try to extend it for the general case.

References

[1] Tapas Mishra and Sudebkumar Prasant Pal. **Bicoloring covers for graphs and hypergraphs**. *arXiv preprint arXiv:1501.00343*, 2015.
[2] Eric Blais, Amit Weinstein, and Yuichi Yoshida. **Semi-strong coloring of intersecting hypergraphs.** *arXiv preprint arXiv:1203.2868*, 2012.

Tirthankar Dasgupta
Email: iamtirthankar@gmail.com
Joined the department in: January 2010

Tirthankar Dasgupta *received a B.E. degree in Information Technology from MCKV Institute of Technology, Kolkata in 2003, and an MS degree in Computer Science from Indian Institute of Technology, Kharagpur in 2009. From January 2009 till December 2009, he worked in Society for Natural Language Technology Research, Kolkata as a Researcher. Since January 2010, he has been a research scholar in the department of Computer Science & Engineering in IIT Kharagpur. His research interests are in the areas of Natural Language Processing, Cognitive Science, psycholinguistics and Assistive Technology.*

Supervisor: Prof. Anupam Basu

Cognitively motivated computational models of representing Bangla morphologically complex words in a lexicon

In this work, we have developed cognitively motivated computational models for the representation and processing of Bangla morphologically complex words (like, derivationally suffixed, compounds and phrasal verbs) in a computational lexicon. To achieve this, we have performed different cross-modal priming experiments to collect data and explore the interaction between different linguistic factors in the possible representation and processing of words in the human mind. Based on the empirical results we have developed and applied different computational models like, frequency and productivity based models, information theoretic measures, vector space models, semantic compositionality and other distributional semantics techniques to model our observations.

Through different psycholinguistic experiments, we have observed that the representation of words depends upon the activation and deactivation of its constituent bound and/or free morphemes. Such activation and deactivations are primarily modulated by the morphological relatedness, orthographic transparencies and semantic compositionality between the words and their constituents. These observations are made by examining the priming effect between the words and their constituents. Further analysis of the reaction time and error rates reveals several interesting facts such as (a) apart from usage frequency, word length and presence of certain orthographical features also affect the representation and processing of a word, (b) in case of derived words, certain derivational suffixes inherited from Sanskrit, which usually make the derived word orthographically or semantically opaque, do not trigger priming; this indicates that these morphological relations are no longer recognized or internalized by the modern Bangla speakers and (c) apart from morphological relatedness, semantic compositionality between the whole word and its constituents also plays an important role in the representation and processing of Bangla morphologically complex words. These and similar other observations make us believe that understanding the precise nature of the mental representation of morphological processes in Bangla (as well as other Indian languages) is a challenging and potent research area that is very little explored.

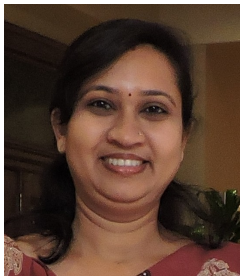
Based on the above empirical experiments we have collected a large sample of reaction time data and incrementally developed a number of frequency based, morphological complexity and semantic compositionality based computational models. Finally, we have combined all these individual models together to develop an enhanced parallel lexical activation model that can predict the possible representation and processing of Bangla words in the mental lexicon. This model is then augmented to

a lexical representation scheme to decide which words should be listed in the lexicon and which one are to be processed on the fly using a morphological analyzer. A representation scheme for the computational lexicon based on the principles of mental lexicon organization is expected to perform better because its success and failure in processing words are expected to meet the expectations of the end user.

References:

[1] Frost, R., Forster, K.I., & Deutsch, A. (1997). What can we learn from the morphology of Hebrew? A masked-priming investigation of morphological representation. Journal of Experimental Psychology: Learning, Memory, and Cognition, 23, 829–856.

[2] Marslen-Wilson, W.D., Tyler, L.K., Waksler, R., & Older, L. (1994). Morphology and meaning in the English mental lexicon. Psychological Review, 101, pp. 3–33.



Tripti Swarnkar
Email: tripti.swarnkar@cse.iitkgp.ernet.in, swarnkar.tripti@gmail.com
Joined the department in: July 2011

Tripti Swarnkar *received an MCA degree from Government Engineering College Raipur C.G. (presently NIT Raipur), in 1998, and an M.Tech. degree in Computer Science from Utkal University, Bhubaneswar Odisa in 2005. From November 1998 till September 1999, worked as Lecturer in Bhilai Institute of Technology (BIT), Bhilai C.G. Joined Institute of Technical Education and Research (ITER), SOA University, Bhubaneswar, Odisa as Lecturer Computer Science & Engineering in October 1999. At present holding the post of Associate Professor in the Department of Computer Application at ITER. Since July 2011, she is a research scholar in the department of Computer Science & Engineering in IIT Kharagpur. Her research interests are in the areas of Bioinformatics and Machine Learning.*

Supervisor: Prof. Pabitra Mitra

Unsupervised Learning for Gene Selection and Enrichment using Microarray Data

A challenge in bioinformatics is to analyze volumes of gene expression data generated through microarray and yield useful information. Consequently, most microarray studies demands complex data analysis to infer biologically meaningful information from such high throughput data. Selection of informative genes for sample classification is an important data analysis step to identify a set of genes which can further help in finding the biological information embedded in microarray data, and thus assists in diagnosis, prognosis and treatment of the disease. The goal of our work is to perform gene subset selection, which are informative signature genes that characterize diseases, and provide insight into underlying biological processes.

Our work focuses on extending existing gene selection methodologies by hybridizing statistical, ontology based and network based approaches. The goal is to address the challenges of multiview representation, improved biological interpretation, and study of related biological processes. The contributions of the work are: (i) to obtain multiview clustering of microarray data sets, we suggest an unsupervised feature selection technique, thereby, facilitating gene subset selection which are informative genes, not just discriminatory, but biologically enriched genes which are responsible for concerned biological processes and may be multi-faceted by nature, (ii) judiciously, integrate multiview clusters of gene expression data with the known protein–protein interaction (PPI) knowledge to obtain enriched gene sets and found that it represent strongly connected regions of the known PPI networks, perhaps corresponding to those responsible for certain biological processes, (iii) integrate expression analysis with structural analysis of gene interaction networks, generating dense subgraphs of gene networks, which are functionally associated, largely similar across independent datasets, and are important for discovery of disease causing genes, and (iv) a data analysis methodology is developed for identification and visualization of co-expressed gene patterns, as emerging clusters, in global transcriptome of epithelial cancer pre-malignant and malignant conditions in comparison to their normal counterparts. It provides an intuitive understanding of molecular course in carcinogenesis and may contribute for combinatorial biomarker discovery.

The investigation shows that integration of prior knowledge of the known gene network with transcriptome data for interaction based gene selection or functional module selection provides better biological interpretation and improved statistical analysis.

Urbi Chatterjee
Email: turbi.chatterjee@cse.iitkgp.ernet.in
Joined the department in: January 2015

Urbi Chatterjee *received his B.Tech. in Computer Science and Engg. from Asansol Engineering College, Asansol in 2011. Then she had opted the M.Tech Program in Indian School of Mines, Dhanbad and completed it in 2013. Since then, she had worked in TATA Consultancy Services Limited as Assistant Systems Engineer. She joined the department of Computer Science & Engineering in Indian Institute of Technology Kharagpur as a Ph.D. scholar in January, 2015. Her broad area of research is Hardware Security.*

Supervisor: Prof. Rajat Subhra Chakraborty and Prof. Debdeep Mukhopadhyay

Implementation of Physically Unclonable Function as Hardware Security Primitive

We set our broad goal for research on designing Security Protocols based on PUF for objects like Internet-of-Things. The Internet of Things (IoT) is the interconnection of distinctively recognizable embedded computing devices within the present Internet infrastructure. Things, in the IoT, can refer to a widespread variety of devices such as heart monitoring implants, biochip transponders on farm animals, electric clams in coastal waters, automobiles with built-in sensors, or field operation devices that assist fire-fighters in search and rescue. According to Gartner, Inc., there will be approximately 26 billion devices on the Internet of Things by 2020.

Now as these devices are pervasive and ubiquitous, they need a trusted computational system which is as small as possible. The Internet Security Protocol currently rests on a well-known and widely trusted set of cryptographic algorithms. The RSA asymmetric algorithm for digital signatures and key exchange; the AES block cipher for confidentiality; the Diffie-Hellman(DH) asymmetric key agreement algorithm; and the SHA-1 and SHA-256 secure hash algorithms. But significant amount of resources such as processor speed and memory are expected for functioning of the application scenario – something which is not always available in the context of IoTs. So we plan to undertake a fresh approach by considering new hardware security primitives which can be easily integrated in the IoT devices. Also, we plan to implement new verification techniques to evaluate the security and functional correctness of the proposed systems.


MS Scholars

Abhishek Chakraborty
Email: abhishek.chakraborty@cse.iitkgp.ernet.in
Joined the department in: December 2013

Abhishek Chakraborty *received his B.Tech. degree in Electronics & Communication Engineering from Institute of Engineering and Management, Kolkata in 2013. Since June 2013, he has been a research scholar in the department of Computer Science & Engineering, IIT Kharagpur. His research interests are in the areas of Cryptography and VLSI design.*

Supervisor: Prof. Debdeep Mukhopadhyay

Power and Fault Analysis Attacks on Stream Ciphers

Cryptographic algorithms are extensively used in the modern era to ensure message confidentiality and integrity, secure computing, authentication of the communicating parties, digital signatures and several other applications. Traditionally, the robustness of cryptographic primitives has been determined using mathematical models and statistical analysis. However, the real life implementations of these ciphers can be studied and analyzed to mount side channel attacks (SCAs). The potential threat of SCA based on information leakage from power consumption, timing variations, and electromagnetic radiations from physical implementation of the cipher system has been well established in the recent past where system breakdown can be achieved with relatively less computational cost compared to the conventional mathematical cryptanalysis.

A stream cipher is a symmetric key cipher where the plaintext digits are combined with a pseudo-random keystream to produce ciphertext digits. My current research interests include power and fault analysis attacks against stream cipher implementations on field-programmable gate arrays (FPGAs).

Abhrajit Sengupta
Email: abhrajit.sengupta@cse.iitkgp.ernet.in, abhrajit.sengupta@gmail.com
Joined the department in: May 2012

Abhrajit Sengupta *is presently an MS scholar in the Department of Computer Science & Engineering at IIT Kharagpur. He received his B.E. in Computer Science & Engineering from Jadavpur University, Kolkata in 2011. Before joining IIT Kharagpur he was associated with Acclaris Business Solutions Pvt. Ltd. as a software engineer. His research interest lies in the areas of cryptography and complexity theory.*

Supervisor: Prof. Dipanwita Roychaudhury

Authentication Schemes Based on Coding Theory

Currently I'm working on constructing a provably secure message authentication code (MAC). Classical authentication schemes, though very fast, can not claim provable security. That may be achieved by following public key design principles, at the cost of being less efficient. But, with the advent of quantum computers, most if not all conventional public-key cryptosystems, namely, systems based on integer factorization (RSA) or the discrete logarithm problem (like traditional or elliptic curve Diffie-Hellman) can potentially be broken. Nonetheless, there are other important classes of cryptographic systems beyond RSA and ECDSA that are believed to resist both classical and quantum analysis. McEliece cryptosystem (or Niederreiter version), invented by R.J. McEliece forms one such class with its security related to the hardness of syndrome decoding from coding theory. Till date there is no polynomial time algorithm beyond the generic improvem ents possible with Grovers technique for decoding a random code, making it an excellent candidate for post quantum cryptography. The aim of our work is to design a provably secure authentication scheme in the symmetric key setting which is also secure in the quantum computing model.

Anirban Ghose
Email: anighose25@gmail.com, anirban.ghose@cse.iitkgp.ernet.in
Joined the department in: January 2014

Anirban Ghose *received his B. Tech degree in Computer Science and Engineering from Heritage Institute of Technology in 2013. From September 2013, he has been working as a Research Consultant in the Department of Computer Science and Engineering, IIT Kharagpur under the project: "Architectural and Algorithmic Optimizations for Speech based communication interfaces in mobile devices." Since, January 2014, he has been a research scholar in the Department of Computer Science and Engineering, IIT Kharagpur.*

Supervisors: Prof. Soumyajit Dey and Prof. Pabitra Mitra

Machine Learning Assisted Compilation Strategies for Heterogeneous CPU-GPU Programs

Heterogeneous architectures promise to deliver high performance at a relatively lower cost when compared to homogeneous systems. However the full potential of such computing systems can be realized only if the computation is mapped effectively to the different cores present in the system. The task of mapping computational workloads between cores in heterogeneous architectures for improved performance has become increasingly prevalent in recent times. OpenCL is a widely used low-level programming framework which allows programmers to assign workloads to different devices across the system. Determining the optimal partitioning for an OpenCL program on a heterogeneous architecture is an extremely difficult job for an application programmer. The goal of the current work is to use machine learning techniques to determine from static code features of the source program to infer the workload distribution ratio for a CPU-GPU system and perform a source to source compiler level transformation to generate a partitioned version for the same. Future work entails incorporating architectural parameters through version revisions of the computing platform. As hardware characteristics continue to evolve over time, the program partitions derived for a particular application are unlikely to remain constant. So it becomes necessary to learn with additional architectural features to determine the optimal partition of OpenCL programs for different target platforms.

Debasmita Lohar
Email: debasmita.lohar@cse.iitkgp.ernet.in, dlohar2009@gmail.com
Joined the department in: January 2014

Debasmita Lohar *received a B.Tech. Degree in Computer Science and Engineering from Heritage Institute of Technology, Kolkata, in 2013. From September 2013, she is working as a Research Consultant in the Department of Computer Science & Engineering, IIT Kharagpur, under the project: "Architectural and Algorithmic Optimizations for Speech based Communication Interfaces on Mobile Devices". Her research interests are in the areas of Embedded Systems, Reliability Analysis, Formal methods, Program Analysis.*

Supervisor: Prof. Soumyajit Dey

Probabilistic Program Analysis for Reliability Analysis

A software is not built with the idea of handling every possible input test case as part of its computational path. If we may assume a correct implementation, such inputs and their executions are taken care of using assertions and exception handlers by the programmer. In a fault tolerant scenario, an assertion failure is typically handled using re-execution or N-version programming. Hence, the probability distribution of the possible inputs for the software and its potential ramifications (dataflow analysis) may possibly reveal the mean time for such assertion failures. Given a program description of a software system model with a probability distribution over the possible inputs for the system, we are interested to compute reliability indices like Mean Time To Failure (MTTF) for the software system using abstract interpretation based static analysis methods. As part of the current research, we are also interested in creating an automated tool flow which can compute these reliability indices for software systems.

A possible application of such probabilistic program analysis may be estimation of control performance for embedded control software which works in noisy environments. In a practical operating environment, sensor data often gets corrupted time to time. A robust controller should be able to handle such intermittent data corruption in a graceful manner. Addition of noise with actual program inputs can simply be considered as a superposition of two probability distribution functions (pdfs) to give a new pdf for the input. Our Analysis method can be used to estimate a controller's robustness in such a scenario.

K SAI RAM
Email: sairam.kasanagottu@gmail.com
Joined the department in: December 2014

K SAI RAM *received a B.Tech(Honors) degree in Electronics and Electrical Communication Engineering in Indian Institute of Technology, Kharagpur in 2014. From July 2014, he worked in Philips India Ltd as an Assistant Manager, Design and Development of LED Lamps for four months. Since December 2014, he has been a research scholar and also pursuing M.S degree in the department of Computer Science & Engineering in IIT Kharagpur. His research interests are in the areas of Robotics and Image Processing.*

Supervisor: Prof. Jayanta Mukhopadhyay and Prof. Patha Pratim Das

Paheli Bhattacharya
Email: pahelibhattacharya@gmail.com
Joined the department in: July 2014

Paheli Bhattacharya *is currently pursuing Master of Science (MS by research) in the Department of Computer Science and Engineering at IIT Kharagpur. She completed her Bachelor of Technology from Govt. College of Engineering and Textile Technology, Serampore (WBUT). She completed by schooling from Auxilium Convent School, Bandel. Her current research is in the domain of Natural Language Processing, Information Retreival and Machine Learning.*

Supervisor: Prof. Pawan Goyal and Prof. Sudeshna Sarkar

Tentative : Modelling Cognate Words in the Indo-European Language System

My research aims to effectively model cognate words in the Indo-European Language System. We aim to propose methods that can automatically identify cognate words over languages. We are working on Indian languages as of now and aim to extend it to the IELS

Prabir Mallick
Email: prabir.mallick9@gmail.com
Joined the department in: July 2014

Prabir Mallick *passed Btech in the year 2010 in Electronics and communication from Heritage Institute of Technology, Kolkata. He worked three years for Wipro Technologies. From july 2014 onwards, he is pursuing MS in computer science in IIT kharagpur.*

Supervisor: Prof. Pabitra Mitra and Prof. Sudeshna Sarkar

Building intelligent freight exchange platform

I am working on building an intelligent freight exchange platform to harness logistics system in india.

Poulami Das
Email: poulamidas22@gmail.com
Joined the department in: February 2014

Poulami Das *received a B.E degree from the Computer Science and Engineering Department, Jadavpur University, Kolkata in the year 2012. From February 2014, she started working as a Research Assistant in the Department of Computer Science and Engineering, IIT Kharagpur, under the project entitled "Indigenous design methodologies of elliptic curve cryptography on FPGAs". Since July,2014 she has been a MS scholar in the Department.*

Supervisor: Prof. Debdeep Mukhopadhyay

Design and Analysis of 'safe' Elliptic Curves

The domain of public key cryptography has been mainly reigned by the RSA cryptosystem[1] since its advent in 1977. Till today it is being widely used in protecting all kinds of important online public transactions. But RSA has the disadvantage of high implementation cost, and hence it becomes difficult to implement it to secure low cost embedded devices with constrained resources. This is when Elliptic Curve Cryptography(ECC)[2] came to the rescue. In the year 1985 Neal Koblitz and Victor S.Miller independently introduced the idea of Elliptic Curve Cryptography explained how Group operation is defined on an elliptic curve which is a cubic curve with non-zero Discriminant. As can be noted that 2048 key bit security in RSA is roughly equivalent to 224 key bit security in ECC, and this advantage of shorter key values in case of ECC opens the path for embedded system designers to secure their implementations with this new alternative.

However, when ECC is implemented in hardware it opens the trapdoor for new vulnerabilities[3]. When an elliptic curve computation takes place, it leaks information in terms of timings (the underlying operations involved in a scalar multiplication are Addition and Doubling operations which take dissimilar times to execute), in terms of power absorption (the amount of power that a running device uses to compute a elliptic curve operation is dependent on the key value an leaks information about the key). So a designer needs to take care of all these side channel vulnerabilities to keep a implementation secure. Again the Addition and Doubling formulas used varies with respect to the form of curve that is being used - till this date quite a number of elliptic curve forms has been introduced - there are NIST standardized curves, GLV form of curves, Edward form of curves and others. We are trying to exploit which curve form is more inherently secure against side channel attacks and which are the elliptic curve parameters(absence of Montgomery ladder, absence of twist security etc)[4] that are more susceptible to leak information about the key in an embedded environment.

[1] Ronald L. Rivest, Adi Shamir, Leonard M. Adleman: A *Method for Obtaining Digital Signatures and Public-Key Cryptosystems*. Commun. ACM 21(2): 120-126 (1978)

[2] Victor S. Miller: *Use of Elliptic Curves in Cryptography*. CRYPTO 1985: 417-426

[3] Jean-Sébastien Coron: *Resistance against Differential Power Analysis for Elliptic Curve Cryptosystems*. CHES 1999: 292-302

[4] http://safecurves.cr.yp.to/

Sankarshan Mridha
Email: sankarshan7@gmail.com
Joined the department in: January 2015

Sankarshan Mridha *received his B.E. degree in Computer Science and Engineering from Jadavpur University, Kolkata in 2013. From August 2013 to July 2014 he was Programmer Analyst Trainee in Cognizant Technology Solutions India Pvt. Ltd. in Kolkata. Since January 2015 he has been an MS research scholar in the department of Computer Science and Engineering in IIT Kharagpur. His research interests are in the area of Machine Learning and Complex Network.*

Supervisor: Prof. Sourangshu Bhattacharya and Prof Niloy Ganguly

Study Negative Opinion of Related Users in Social Network

Social networks are characterized by the opinions of different people about different topics ranging from political issues to social service, entertainment to sports, national events to international stories. People have various kinds of opinions and they are very very diverse in nature. These opinions are positive and as well as negative in nature. Now negative opinion has a key role in building social interaction structure. People's interaction with each other changes due to the impact of negative opinion which changes the network structure.

This work aims to study the negative opinion of related users and to predict about the change in interaction pattern among them.

Sayandeep Saha
Email: sahasayandeep91@gmail.com
Joined the department in: December 2013

Sayandeep Saha *received a B.Tech. degree in Information Technology from Institute of Engineering and Management, Kolkata in 2013. Since December 2013, he has been a research scholar pursuing MS degree in the Department of Computer Science & Engineering in Indian Institute of Technology, Kharagpur. His research interests are in Hardware & Network Security, and Cryptography. He is associated with the Secured Embedded Architecture Laboratory (SEAL), CSE Department.*

Supervisors: Prof. Rajat Subhra Chakraborty and Prof. Debdeep Mukhopadhyay

Hardware Based Attacks on Cryptographic and Network Devices

In our research, we primarily focus on the security threats for cryptographic devices as well as networks, originating from either their design and implementation, or from the untrusted manufacturing chain they pass through. The scope of some malicious modifications of a circuit within the IC manufacturing chain has become a serious threat, as they can lead to device malfunctions or leakage of secret information. These malicious modifications are called Hardware Trojan Horses (HTH). HTHs are stealthy in nature and thus cannot be detected by conventional IC testing methodologies. Thus more sophisticated and targeted testing techniques are required which is one goal of our research. Moreover, the investigation of newer attack models and methodologies using HTHs is another major aspect. Currently we focus on FPGA based circuit implementations as their programmability makes them more vulnerable to HTHs.

A slightly different direction of this research includes the utilization of HTHs for side-channel attacks on cryptographic and network devices. Investigating their catastrophic effects on public networks and widely accepted crypto implementations is our prime target. Finally, we also propose some hardware-intrinsic countermeasures one of which is Physically Unclonable Functions (PUF). The unclonable feature of PUFs makes them a popular choice for the purpose of authentication and anti-counterfeiting for hardwares. Our aim is to formalize the behavior of PUFs through mathematical frameworks so that they can be efficiently utilized for device security.

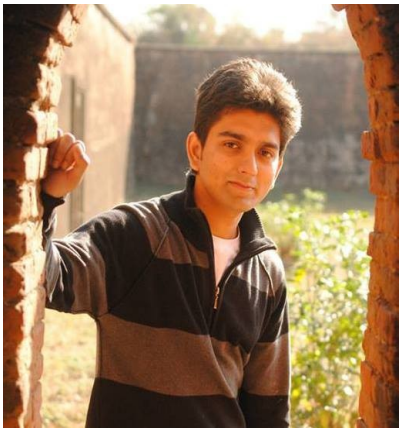
Shamit Ghosh
Email: shamit.ghosh@cse.iitkgp.ernet.in, raaz714@gmail.com
Joined the department in: July 2012

Shamit Ghosh *received his B.E. degree in Computer Science & Engineering from Jadavpur University, Kolkata in 2011. From 20th June, 2011 to 30th April, 2012 he worked as a Software Developer at Rancore Technologies, RIL-4G project. He joined as an MS scholar in the department of Computer Science & Engineering in IIT Kharagpur in June 2012. His current research interests are in Side Channel attacks on Block Cipher, Cellular Automata and Fault Attack countermeasures.*

Supervisor: Prof. Dipanwita Roychaudhury

Fault Attack Countermeasure on Symmetric Ciphers

Fault attack is one of the most popular side channel attack. The invention of easier fault injection techniques makes it highly feasible. Many of the existing symmetric ciphers, though algebraically secure, has been cryptanalyzed using fault attacks. The principal focus of my work is to formalize fault attack techniques and to device countermeasures against them.



Shiladitya Ghosh
Email: shiladitya.ghosh@cse.iitkgp.ernet.in, shiladitya321@gmail.com
Joined the department in: December 2013

Shiladitya Ghosh *received his B.Tech. in Computer Science and Engineering from St. Thomas College of Engineering and Technology, Kolkata in 2011. Since, he had been working with Infosys Ltd till December, 2013. He joined the department of Computer Science & Engineering in Indian Institute of Technology Kharagpur as a research scholar in January, 2014. His broad area of research is Formal analysis and design with application in the field of Railways interlocking and Cyber-physical systems.*

Supervisors: Prof. Chittaranjan Mandal and Prof. Pallab Dasgupta

Formal Modelling and Validation of Railway Interlocking

In railway electronic interlocking system, the automatic signalling equipment is programmed with the configuration data derived manually from the yard layout. This step is prone to human errors and any error can be a severe threat to signalling safety. The yard-layout data and the configured system both need to be verified to satisfy the desired safety requirements. The verification process requires the construction of formal model based on yard-layout data and the dependencies listed in control table. It is then necessary to check that relevant safety properties are satisfied by the model. The safety requirements are specified as part of the Railway signalling principles. The signalling principles follow standards accepted universally across different railways. Presently my work focuses on interpreting these safety requirements as temporal properties and verify if the interlocking system of a yard adheres to specifications or not. For verification Bounded Model Checking is used. The proof of concept has already been established with real-life data from a couple of railway yards. In addition to this, I am also working towards verification of train control systems, which the Indian Railway plans to adopt from the European Train Control Systems (ETCS).

Sonam Singh
Email: sonamsingh19@gmail.com
Joined the department in: July 2014

Sonam Singh c*ompleted B.Tech in 2010 from UPTU in Computer Science. After that, he worked at IBM India as SAP developer for a while before moving on to pursue my academic research interests in data mining. He has worked as research assistant at University of Applied Sciences, Berlin on platform for data as a service for more than a year and currently pursuing MS. from IIT kharagpur in climate informatics.*

Supervisors: Prof. Sudeshna Sarkar and Prof. Pabitra Mitra

Climate data modelling using machine learning

Climate data has seen tremendous growth due to products available from satellites and in-situ observations in the field. Making sense of this data is fundamentally challenging not only because of the scale but also because of heterogeneity and domain knowledge required to validate the results. Traditionally, physical modeling has been at the core of climate modeling but recent data mining approaches have shown tremendous potential to uncover relation among known phenomenon to model and predict various global and local events. Recent studies of climate change with machine learning have established the strong need to research in climate informatics. We are researching along these lines on application of machine learning approaches for various interesting events on climate data: prediction of rainfall, feature extraction from Doppler Data and ground water prediction in Indian context etc.

Sulagna Gope
Email: sulagna.student12@gmail.com
Joined the department in: July 2014

Sulagna Gope r*eceived B.Tech degree in CSE from Heritage Institute of Technology, Kolkata. She joined the institute in July 2014 as a research scholar. Her research interest are in areas of Machine learning and datamining.*

Supervisors: Prof. Sudeshna Sarkar and Prof. Pabitra Mitra

Extreme Rainfall Prediction Using Machine Learning Techniques

Prediction of extreme rainfall is a very challenging task, specially in urbanised regions like Mumbai, Kolkata, etc in India. Every year these regions get flooded which cause human and economic losses. Early prediction can help in dislocating people and taking all necessary precautions to prevent the severe impacts. The present models that are used for the prediction are mainly numerical models. These models fail to predict extreme events far ahead of time. Thus precautions could not be taken at appropriate time. They also generate a large number of false alarms.

We are trying to implement Machine Learning techniques like SVM, etc. to predict extreme events. Our target is to give accurate predictions, much before the occurrence of the events.

Our Mentors: Faculty of the Department

Abhijit Das
Email: abhij@cse.iitkgp.ernet.in

Research Interests: *Arithmetic and algebraic computations with specific applications to cryptology*

Abhijit Das is an Associate Professor in the Department of Computer Science & Engineering, Indian Institute of Technology Kharagpur. Before joining IITKGP, he held academic positions at the Indian Institute of Technology Kanpur and Ruhr-Universität Bochum, Germany. Dr. Das received his BE degree from Jadavpur University, Calcutta in 1991, and ME and PhD degrees from Indian Institute of Science, Bangalore, in 1993 and 2000, respectively. His research interests include arithmetic and algebraic algorithms and their parallel implementations, with specific applications to cryptology. He is the author of two graduate textbooks: “Public-Key Cryptography: Theory and Practice” (Pearson Education, 2009, coauthored by Prof. C. E. Veni Madhavan, IISc Bangalore) and “Computational Number Theory” (CRC, 2013).

Ajit Pal
Email: apal@cse.iitkgp.ernet.in

Research Interests: *Embedded systems, low-power VLSI circuits, sensor networks and optical communication*

Ajit Pal is currently a Professor in the Department of Computer Science and Engineering at Indian Institute of TechnologyKharagpur. He received his M.Tech. and Ph.D. degrees from the Institute of Radio Physics and Electronics, Calcutta niversity in 1971 and 1976, respectively. Before joining IITKGP in the year 1982, he was with Indian Statistical Institute (ISI), Calcutta, Indian Telephone Industries (ITI), Naini and Defense Electronics Research Laboratory (DLRL), Hyderabad in various capacities. He became full Professor in 1988 and served as Head of Computer Center from 1993 to 1995 and Head of the Computer Science and Engineering Department from 1995 to 1998. His research interests include Embedded Systems, Low-power VLSI Circuits, Sensor Networks and Optical Communication. He is the principal investigator of several Sponsored Research Projects including “Low Power Circuits” sponsored by Intel, USA and “Formal methods for power intent verification,” sponsored by Synopsis (India) Pvt. Ltd. He has over 150 publications in reputed journals and conference proceedings and three books entitled “Microprocessors: Principles and Applications” published by TMH (1990), “Microcontrollers: Principles and Applications” published by PHI (2011) and “Data Communication and Computer Networks” by PHI (2014). Another book entitled “Low Power VLSI Circuits and Systems” to be published shortly by Springer. He is the Fellow of the IETE, India and Senior Member of the IEEE, USA.

Animesh Mukherjee
Email: animeshm@cse.iitkgp.ernet.in

Research Interests: *Complex systems, language dynamics, social computation, web social media*

Animesh Mukherjee is an assistant professor at the Department of Computer Science and Engineering, IIT Kharagpur and a Simons Associate, ICTP, Trieste, Italy. He completed his doctoral degree from

the same department and then moved to ISI Foundation, Torino, Italy as a post-doctoral researcher. His areas of interest center around studying various complex sociocultural phenomena (e.g., linguistic ability, scientific productivity) under the lens of statistical physics as well computer science. Dr. Mukherjee received the prestigious Young Scientist award from the Indian Science Congress Association in 2006, the Young Engineer Award from the Indian National Academy of Engineering in 2012 and the Young Scientist Medal from the Indian National Science Academy in 2013. He has authored more than 50 research articles (journals and refereed conferences) and co-edited two books from Birkhauser and a special issue of the Computer Speech and Language Journal. He actively serves as member technical programme committee for various top-notch conferences and as a referee/member editorial board for various journals of repute.

Anupam Basu

Email: anupam@cse.iitkgp.ernet.in

Research Interests: *Emdedded systems, cognitive science and language processing with particular focus on intelligent interface design and human computer interaction*

Prof. Anupam Basu is a Professor at the Dept. of Computer Science & Engineering, IIT Kharagpur, and India. He has been in the faculty since 1984. His research interests include Intelligent Systems, Embedded Systems and Language Processing. His research has been directed to develop a number of cost effective Assistive Systems for the physically challenged as well as for development educational systems for the rural children. In all these applications, he has synthesized his research to lead to products, which are presently in use in several village knowledge centers as well as in several organizations for the physically challenged. He is considered to be a pioneer in Assistive Technology research in India.

Presently, he is also serving as the Director of the Society for Natural Language Technology Research, an R& D institute aimed at carrying out language localization research and development.

Prof. Basu had taught at the University of Guelph, Canada, University of California, and Irvine and at the Dortmund University, Germany. He is an Alexander von Humboldt Fellow and a Fellow of the Indian National Academy of Engineering.

He has won several awards and honors for his research contributions. These include the National Award for the Best Technology Innovation for the Physically Disabled (2007), the Da Vinci Award 2004, and Outstanding Young Person Award 1996.

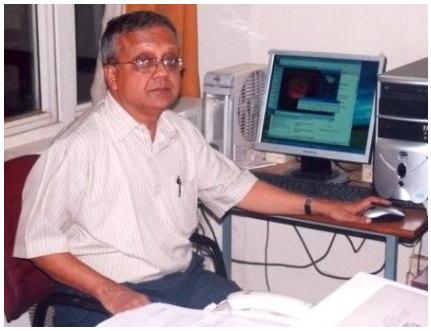
Arobinda Gupta

Email: agupta@cse.iitkgp.ernet.in

Research Interests: *Distributed systems, networks*

Arobinda Gupta received his Ph.D. in Computer Science from the University of Iowa, Iowa City, in 1997, an M.S. in Computer Science fromthe University of Alabama in 1992, and an M.E. and a B.E. in Electronics and Telecommunication Engineering from the Jadavpur University, Kolkata, India in 1990 and 1987 respectively. From February 1990 to September 1999, he was with the Windows 2000 Distributed Infrastructure group in Microsoft Corp., Redmond,

Washington, USA. Since Oct. 1999, he is a faculty in Indian Institute of Technology Kharagpur, where he is currently a Professor in the Department of Computer Science & Engineering. His current research interests are broadly in the areas of distributed systems and networks.



Arun Kumar Majumdar
Email: akmj@cse.iitkgp.ernet.in

Research Interests: *Data and knowledge-based systems, multimedia systems, medical informatics, VLSI design automation*

A. K. Majumdar obtained B. Tech, M. Tech and Ph. D. degree in Applied Physics from the University of Calcutta in 1967, 1968 and 1973, respectively. He also obtained a Ph. D. degree in Electrical Engineering from the University of Florida, Gainesville, U. S. A., in 1976. Since 1980, he is associated with the Indian Institute of Technology, Kharagpur, first as an Assistant Professor in the Electronics and Electrical Communication Engineering Department and then from 1984 as a Professor in the Computer Science and Engineering Department. With leave from IIT, Kharagpur, he served as a Visiting Professor in the University of Guelph, Ontario, Canada in 1986-87, and in the George Mason University, Fairfax, Virginia, USA, in the summer of 1999. Earlier, he worked in the Indian Statistical Institute, Calcutta, and Jawaharlal Nehru University, New Delhi, as a faculty member. He is currently the Deputy Director, IIT Kharagpur. He has also served as Head, School of Medical Science & Technology, IIT Kharagpur, from 2005 to 2006, Dean (Faculty and Planning), IIT Kharagpur from March 2002 to 2005, Head of the Computer Science and Engineering Department, IIT Kharagpur from 1992 to 1995 again from 1998 to May 2001 and Head of Computer and Informatics Center, IIT Kharagpur: from 1998 to 2002.

Bivas Mitra
Email: bivas@cse.iitkgp.ernet.in

Research Interests: *Technological network modeling, complex and dynamic networks, interdependent networks, mobile networks*

Bivas Mitra is an Assistant Professor in the Dept. of Computer Science & Engineering at IIT Kharagpur, India. He earned his Ph.D in Computer Science and Engineering from IIT Kharagpur in 2011. During PhD tenure, he was the recipient of National Doctoral Fellowship and SAP Labs India Doctoral Fellowship, etc. After PhD, he worked as a postdoctoral researcher for two years (May 2010– July 2012) at the French National Centre for Scientific Research (CNRS), Paris, France and Universite catholique de Louvain (UCL), Belgium. He also spent a short stint in industry with Samsung Electronics, Noida as a Chief Engineer. Dr. Mitra is associated with the Complex Networks Research Group (CNeRG), IIT Kharagpur, India. His research interests include complex and dynamical networks, social networks and mobile networks.

Chittaranjan Mandal

Email: chitta@cse.iitkgp.ernet.in

Research Interests: *Formal modelling and verification, high-level design, network and web technologies*

Chittaranjan Mandal received his Ph.D. degree from IIT, Kharagpur, India, in 1997. He is currently a Professor with the Department of Computer Science and Engineering and also the School of Information Technology, IIT, Kharagpur. Earlier he served as a Reader with Jadavpur University. His research interests include formal modelling and verification, high-level design and network and web technologies. He has about seventy publications and he also serves as a reviewer for several journals and conferences. Prof. Mandal has been an Industrial Fellow of Kingston University, UK, since 2000. He was also a recipient of a Royal Society Fellowship for conducting collaborative research. He has handled sponsored projects from government agencies such as DIT, DST and MHRD and also from private agencies such as Nokia, Natsem and Intel.

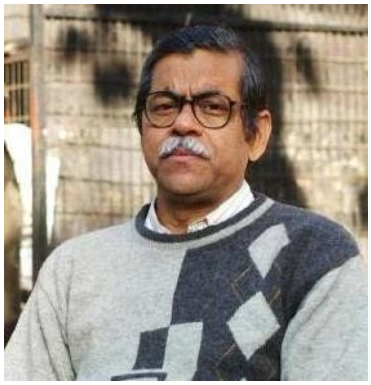
Debdeep Mukhopadhyay

Email: debdeep@cse.iitkgp.ernet.in

Research Interests: *Cryptography, side channel analysis, VLSI of cryptographic algorithms, cellular automata*

Debdeep Mukhopadhyay received his BTech degree from the Department of Electrical Engineering, IIT Kharagpur, India. Subsequently, he obtained his MS and PhD from Computer Science and Engineering, IIT Kharagpur. He has worked as an assistant professor in the Department of Computer Science and Engineering, IIT Madras and is presently working as an associate professor in the Department of Computer Science and Engineering, IIT Kharagpur. His research interests include Cryptography, VLSI of Cryptographic Algorithms and Side Channel Analysis. He is currently visiting NYU-Poly under Indo-US Fellowship (IUSSTF 2012).

He is the recipient of the Indian Semiconductor Association (ISA) TechnoInventor award for best PhD thesis (2010), Indian National Science Academy (INSA) Young Scientist Award (2010), Indian National Academy of Engineers (INAE) Young Engineer Award (2010), Associate of Indian Academy of Science (2011), outstanding Young Faculty fellowship from IIT Kharagpur (2011), and IUSSTF fellowship (2012).



Dipankar Sarkar

Email: ds@cse.iitkgp.ernet.in

Research interests: *Formal verification and symbolic reasoning*

Dipankar Sarkar did his B.Tech., M.Tech. in Eletronics and Electrical Communication Engg. and PhD in Engineering from IIT Kharagpur. He has served IIT Kharagpur as faculty member since 1981.

Dipanwita Roy Chowdhury
Email: drc@cse.iitkgp.ernet.in

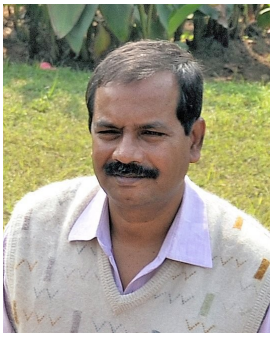
Research Interests: *Design and analysis of cryptographic algorithms, theory and application of cellular automata, and VLSI design and testing*

Dipanwita Roy Chowdhury is a Professor in the Department of Computer Scienece and Engineering, Indian Institute of Technology, Kharagpur, India. She received her B.Tech and M.Tech. degrees in Computer Science from University of Kolkata in 1987 and 1989 respectively, and the PhD degree from the department of Computer Science & Engineering, Indian Institute of Technology, Kharagpur, India in 1994. Her current research interests are in the field of Cryptography, Error Correcting Code, Cellular automata and VLSI Design & Testing. She has published more than 140 technical papers in International Journals and Conferences. Dr. Roy Chowdhury has supervised 11 PhD and 8 MS thesis and she is the Principal Investigator of several R&D projects. She is the recipient of INSA Young Scientist Award and Associate of Indian Academy of Science. She is a fellow of the Indian National Academy of Engineering (INAE).

Indranil Sengupta
Email: isg@cse.iitkgp.ernet.in

Research Interests: *Cryptography and network security, VLSI design and testing, mobile computing*

Dr. Indranil Sengupta obtained his B.Tech., M.Tech. and Ph.D. in Computer Science and Engineering from the University of Calcutta. He joined Indian Institute of Technology Kharagpur, as a Lecturer in 1988, in the Department of Computer Science and Engineering, where he is presently a Professor. He served as Head of the Computer Science and Engineering Department and the School of Information Technology of IIT Kharagpur. A Centre of Excellence in Information Assurance has been set up at IIT Kharagpur under his leadership, where a number of security related projects are executed. He has over 24 years of teaching and research experience, and over 100 publications in international journals and conferences. His research interests include cryptography and network security, VLSI design and testing, and mobile computing.



Jayanta Mukhopadhyay
Email: jay@cse.iitkgp.ernet.in

Research Interests: *Image and video processing, pattern recognition, and multimedia systems*

Dr. Jayanta Mukhopadhyay (Mukherjee) received his B.Tech., M.Tech. and Ph.D. degrees in Electronics and Electrical Communication Engineering from the Indian Institute of Technology (IIT), Kharagpur in 1985, 1987, and 1990, respectively. He joined the faculty of the Department of Electronics and Electrical Communication Engineering at IIT Kharagpur in 1990 and later moved to the Department of Computer Science and Engineering where he is presently a Professor. He served as the head of the Computer and Informatics Center at IIT Kharagpur from September 2004 to July 2007. He also served as the head of the Department of Computer Science and Engineering and the School of Information Technology from April 2010 to March 2013. He was a Humboldt Research Fellow at the Technical University of Munich in Germany for one year in 2002. He also held short

term visiting positions at the University of California, Santa Barbara, University of Southern California, and the National University of Singapore. His research interests are in image processing, pattern recognition, computer graphics, multimedia systems and medical informatics. He published about 200 research papers in journals and conference proceedings in these areas. He received the Young Scientist Award from the Indian National Science Academy in 1992. Dr. Mukherjee is a Senior Member of the IEEE, and a fellow of the Indian National Academy of Engineering (INAE).

Niloy Ganguly

Email: niloy@cse.iitkgp.ernet.in

Research Interests: *Peer-to-peer networks, complex network theory, social networks modeling*

Niloy Ganguly is an associate professor in the department of computer science and engineering, Indian Institute of Technology Kharagpur. He has received his PhD from Bengal Engineering and Science University, Calcutta, India and his Bachelors in Computer Science and Engineering from IIT Kharagpur. He has been a post doctoral fellow in Technical University of Dresden, Germany where he has worked in the EU-funded project Biology-Inspired techniques for Self-Organization in dynamic Networks (BISON). He presently focuses on dynamic and self organizing networks especially peer-to-peer networks, online social networks(OSN), delay tolerant network etc. He has worked on various aspects of OSN like understanding the importance of link farming in OSN and how to discover experts in OSN. In peer-to-peer networks he has worked on optimizing various services like search, topology management and applications like IP telephony, publish subscribe system etc. He has also simultaneously worked on various theoretical issues related to dynamical large networks often termed as complex networks. In this line he has been instrumental in organizing the workshop series Dynamics on and of Complex Networks in European Conference on Complex Systems. He has published around 100 papers in international conferences and journals. He has also edited a book on Complex Networks published by Birkhauser, Boston. He currently publishes in various top ranking international journals and conferences including ACM CCS, PODC, SIGCOMM, ACL, WWW, INFOCOM, Euro Physics Letters, Pysical Review E, ACM and IEEE Transactions, etc. For more information, please visit:

http://www.facweb.iitkgp.ernet.in/~niloy/

Pabitra Mitra

Email: pabitra@cse.iitkgp.ernet.in

Research Interests: *Machine learning, information retrieval, data mining*

Pabitra Mitra did his PhD from Indian Statistical Institute Calcutta in 2003. His research interests are in the fields of machine learning, data mining, information retrieval, and pattern recognition. He has authored a book on Data Mining and about twenty papers in international journals. He is a recipient of the Indian National Academy of Engineering Young Engineer Award in 2007. His hobbies are painting and reading story books.

Pallab Dasgupta

Email: pallab@cse.iitkgp.ernet.in

Research Interests: *Formal verification, artificial intelligence, and VLSI*

Dr. Pallab Dasgupta did his B.Tech, M.Tech and PhD in Computer Science from the Indian Institute of Technology Kharagpur. He is currently a Professor at the Dept. of Computer Sc. & Engg, I.I.T. Kharagpur. His research interests include Formal Verification, Artificial Intelligence and Design AutomationI. He has over 160 research papers and 3 books in these areas.

Prof. Dasgupta specializes in formal methods for proving the correctness of engineering designs. He has contributions in developing and applying formal methods on a wide range of domains, including digital integrated circuits (in partnership with Intel and Synopsys), analog integrated circuits (in collaboration with National Semiconductors, SRC, and Freescale), automotive control (with General Motors), railway signaling (with Indian Railways), and network access control. Dr Dasgupta has been a recipient of the Young Scientist awards from the Indian National Science Academy, Indian National Academy of Engineering and the Indian Academy of Science. He is a Fellow of the Indian National Academy of Engineering, and a Fellow of the Indian Academy of Sciences. Dr. Dasgupta is currently holding the position of Associate Dean of Sponsored Research and Industrial Consultancy (SRIC), IIT Kharagpur.

Partha Bhowmick

Email: pb@cse.iitkgp.ernet.in

Research Interests: *Digital geometry, shape analysis, computer graphics*

Partha Bhowmick graduated from Indian Institute of Technology Kharagpur, India, and received his Masters and PhD from Indian Statistical Institute, Kolkata, India. He is currently an Associate Professor in Computer Science and Engineering Department, Indian Institute of Technology, Kharagpur, India. His research focus primarily is digital geometry, but he works also in algorithmic art, combinatorial image analysis, and computer graphics. He has coauthored over 90 research papers in these areas, which have been published in peer-reviewed international journals, edited volumes, and international conference proceedings. He has also co-authored one book in digital geometry, and he holds 3 US patents.

Partha Pratim Chakrabarti

Email: ppchak@cse.iitkgp.ernet.in

Research Interests: *Artificial intelligence, algorithms for design automation in VLSI and embedded* systems

Partha Pratim Chakrabarti is a Professor in the Department of Computer Science and Engineering at Indian Institute of Technology Kharagpur. Currently, he is holding the post of the Director of IIT Kharagpur. He also held the positions of Dean, Scientific Research and Industrial Consultancy (SRIC), and of Head of the Advanced Technology

Development Centre (ATDC). He received the Bachelor's degree in Computer Science from IIT Kharagpur, India, in 1985. He received Ph.D. in Computer Science & Engineering from IIT Kharagpur. His specific interests include Heuristic and Exploratory Search Techniques, Automated Problem Solving and Reasoning, Algorithms for Synthesis and Verification of VLSI Systems, Scheduling, Verification and Fault Tolerance Analysis of Multi-Processor Embedded Systems, etc. He has over 200 publications, and has supervised around 16 Ph.Ds. He is the principal investigator of several research projects, and is a consultant to industry and government. He helped found the Advanced VLSI Design Laboratory and the General-Motors-IIT-Kharagpur Collaborative Research Laboratory on ECS at IIT Kharagpur. AsDean SRIC, he has helped grow the sponsored research at IIT Kharagpur multiple-fold including setting up of several Advanced Research Centres of Excellence and the Entrepreneurship Programme. He is a Fellow of Indian National Science Academy, Indian Academy of Science, Indian National Academy of Engineering and The West Bengal Academy of Science & Technology. He is the recepient of several awards, including the President of India Gold Medal, Shanti Swarup Bhatnagar Award, Swarnajayanti Fellowship, INSA Young Scientist Award, Indian National Academy of Engineering (INAE) Young Engineer Award, Anil Kumar Bose Award from INSA, Best Paper Awards in International Conference on VLSI Design and National Scholarship.

Partha Pratim Das
Email: ppd@cse.iitkgp.ernet.in

Research Interests: *Human Activity Recognition, Image Processing and Computer Vision, Object-Oriented Analysis and Design, Software Engineering, Compiler Technology, Digital Geometry, and Embedded Systems.*

Dr. Partha Pratim Das received his BTech, MTech and PhD degrees in 1984, 1985 and 1988 respectively from IIT Kharagpur. He served as a faculty in Department of Computer Science and Engineering, IIT Kharagpur from 1988 to 1998 and guided 5 PhDs. In 1998, he joined Alumnus Software Ltd as a Business Development Manager. From 2001 to 2011, he worked for Interra Systems, Inc as a Senior Director and headed its Kolkata Center. In 2011, he joined back to Department of Computer Science and Engineering, IIT Kharagpur as Professor. He is currently the Head of Rajendra Mishra School of Engineering Entrepreneurship at IIT. Dr. Das has also served as a Visiting Professor with Institute of Radio Physics & Electronics, Calcutta University from 2003 to 2013.

Dr. Das has received several recognitions including UNESCO/ROSTSCA Young Scientist (1989), INSA Young Scientist Award (1990), Young Associate-ship of Indian Academy of Sciences (1992), UGC Young Teachers' Career Award (1993), INAE Young Engineer Award (1996), Interra Special (Process) Recognition (2009), and Interra 10 Years' Tenure Plaque (2011). He served as General Chair for International Conference on VLSI Design & Embedded Systems in 2005 and in various capacities for International Symposium on VLSI Design & Test in 2007, 2008 and 2012. He is currently the Editor-in-Chief of The Journal of Institution of Engineers: Series B, reviewer for Pattern Recognition Letters and a Review Writer for ACM Computing Reviews. He is also the Program Chair (Embedded Systems Track) for International Conference on VLSI Design & Embedded Systems scheduled to be held in 2016.

Dr. Das has published over 40 technical papers in international journals in areas of Digital Geometry, Image Processing, Parallel Computing and Knowledge-based Systems. In 2013 he has co-authored a research monograph titled "Digital Geometry in Image Processing" (CRC Press). His current interests include Image Processing and Computer Vision (human activity tracking using Kinect), Object-Oriented Systems Analysis and Design (UML, Design Patterns and C++11), Software Engineering (automated program analysis using static and dynamic instrumentation), Compiler Technology (multi-

threaded debugging), Digital Geometry, and Embedded Systems.

Dr. Das is a member of Association of Computing Machinery (ACM), The Institute of Electrical & Electronics Engineers (IEEE), Indian Unit for Pattern Recognition and Artificial Intelligence (IUPRAI) and VLSI Society of India (VSI).

Partha Sarathi Dey
Email: psd@cse.iitkgp.ernet.in

Research Interests: *Digital logic design, data structures, computer organization and architecture*

M.Tech.(IIT Kharagpur)
Lecturer, Computer Science & Engineering
P S Dey joined the Institute in 1985

Pawan Goyal
Email: pawang@cse.iitkgp.ernet.in

Research Interests: *Computational linguistics, information retrieval, digital humanities, semantic computing*

Pawan Goyal joined the Department of Computer Science and Engineering, Indian Institute of Technology Kharagpur as an Assistant Professor in July 2013. Prior to that, he worked at INRIA Paris-Rocquencourt as a post doctoral fellow with Prof. Gérard Huet on The Sanskrit Heritage Site.

Dr. Goyal did his B. Tech. in Electrical Engineering from Indian Institute of Technology, Kanpur. He received his Ph.D. from Intelligent Systems Research Centre, Faculty of Computing and Engineering, University of Ulster, UK. His PhD advisors were Prof. Laxmidhar Behera and Prof. T. M. McGinnity. The topic of his PhD dissertation was “Analytic Knowledge Discovery Techniques for Ad-Hoc information Retrieval and Text Summarization.”

His main research interests include Sanskrit Computational Linguistics, Natural Language Understanding, Information Retrieval and Digital Humanities.

Pralay Mitra
Email: pralay@cse.iitkgp.ernet.in

Research Interests: *Computational biology and bioinformatics*

Pralay Mitra received the Bachelor of Science (Physics as a major) and Bachelor of Technology (Computer Science and Engineering) from University of Calcutta in 1999 and 2002 respectively. After finishing his Master of Engineering (Computer Science and Information Technology) from Bengal Engineering and Science University, Shibpur, he joined Indian Institute of Science, Bangalore. In 2010, he awarded Ph.D. from the Indian Institute of

Science, Bangalore.

Dr. Mitra is attached with this department as an Assistant Professor since 2013. Before that he was the Senior Research Fellow (2011-2013) at the University of Michigan Medical School, Ann Arbor and the Research Associate (2010-2011) of the Indian Institute of Science, Bangalore. He also worked (2004-2005) in the Avisere Technology Pvt. Ltd as a Senior Computer Engineer.

Dr. Mitra is totally focused on Computational Biology and Bioinformatics. Particularly, he is interested to realizing the biological phenomenon by developing sophisticated computational tools. Towards this end, he developed methods for predicting protein-protein interactions, for assembling macromolecules and for designing novel protein sequences. He is also actively engaged in the development of the computational methods for whole cell simulation.

Rajat Subhra Chakraborty
Email: rschakraborty@cse.iitkgp.ernet.in

Research Interests: *Hardware security, VLSI design, and digital content protection through watermarking*

Rajat Subhra Chakraborty is an Assistant Professor in the Computer Science and Engineering Department of IIT Kharagpur. He received his PhD degree in Computer Engineering from Case Western Reserve University (Cleveland, Ohio, USA) in 2010 and a B.E. (Hons.) in Electronics and Telecommunication Engineering from Jadavpur University in 2005. From 2005-2006, he worked as a CAD Software Engineer at National Semiconductor in Bangalore, and in Fall 2007, he was a co-op at Advanced Micro Devices (AMD) in Sunnyvale, California. He has received multiple student awards from IEEE and ACM, and an annual award for academic excellence among graduate students from Case Western Reserve University in 2009. Part of his PhD research work has been the subject of a U.S. patent filed by Case Western Reserve University in 2010. His research interest includes hardware security, including design methodology for hardware IP/IC protection, hardware Trojan detection/prevention through design and testing, attacks on hardware implementations of cryptographic algorithms and digital-watermarking. He is one of the recipients of IBM Faculty Awards (2012), and recipient of the RECI Fellowship from Royal Academy of Engineering (U.K.) (2014).

Rajeev Kumar
Email: rkumar@cse.iitkgp.ernet.in

Research Interest: *Programming languages and software engineering, embedded and multimedia systems, evolutionary computing*

Rajeev Kumar received his Ph.D. from University of Sheffield and M.Tech. from University of Roorkee (now, IIT Roorkee) both in computer science and engineering. Currently, he is a professor of computer science and engineering at IIT Kharagpur. Prior to joining IIT, he was with the Birla Institute of Technology & Science (BITS), Pilani and the Defense Research and Development Organization (DRDO). His research interests include programming languages & software engineering, embedded & multimedia system, and evolutionary computing for combinatorial optimization. He has supervised 8 Ph.Ds and published over 150 research articles. He is a senior member of ACM and IEEE, and a fellow of IETE.

Rajib Mall
Email: rajib@cse.iitkgp.ernet.in

Research Interest: *program analysis and testing*

Rajib Mall has been with the Computer Science and Engineering at IIT, Kharagpur since in 1994. Dr. Mall is the current head of the department. Prior to joining IIT, Kharagpur, he worked with Motorola India for about three years. Dr. Mall completed all his professional education: Ph.D., Master's, and Bachelor's degrees from the Indian Institute of Science, Bangalore. He has guided 12 Ph.D. dissertations and has authored two books. He has published more than 150 research papers in International refereed conferences and Journals. Dr. Mall works mostly in the area of program analysis and testing.

Rogers Mathew
Email: rogers@cse.iitkgp.ernet.in

Research Interest: *Graph theory, combinatorics, graph algorithms*

Rogers Mathew received a B.Tech. degree from College of Engineering, Trivandrum, India in 2003, an M.E. degree in Computer Science from Indian Institute of Science, Bangalore, India in 2007 and PhD from the same department in 2012. Post PhD, he has worked as a Post Doctoral Fellow in the Dalhousie University, Halifax, Canada (2012-2013) and University of Haifa, Israel (October 2013-November 2015). He joined the Dept. of CSE, IIT Kgp in January 2015.

Sandip Chakraborty
Email: sandipc@cse.iitkgp.ernet.in

Research Interests: *Computer Systems and Networks, Mobile Computing, Distributed Computing*

Sandip Chakraborty is interested broadly in Systems and Networking, with a particular focus on high throughput wireless networks, mobile and Smart-phone networks, network performance modeling and optimization and distributed computing over networks. He received his PhD from Indian Institute of Technology Guwahati in 2014, with the thesis on *Capacity Enhancement, QoS and Rate Adaptation in IEEE 802.11s: A Performance Improvement Perspective*. He has designed and developed *IITGMesh: A High Throughput Mesh Networking Testbed* at IIT Guwahati.

At present, he is an Assistant Professor in the Department of Computer Science and Engineering, Indian Institute of Technology Kharagpur. Prior to that, he has worked as a Visiting Assistant Professor in Indian Institute of Information Technology Guwahati.

Soumyajit Dey
Email: soumya@cse.iitkgp.ernet.in

Research Interests: *Formal methods in system design, computer architecture, assistive technologies*

Soumyajit Dey received a B.E. degree in Electronics and Telecommunication Engg. from Jadavpur University, Kolkata in 2004, an M.S. degree in Computer Science from Indian Institute of Technology, Kharagpur in 2007 and PhD from the same department in 2011. Post PhD, he has worked as Research Associate in the School of Computing, National University Singapore in Autumn 2011. He has also worked at IIT Patna as assistant professor in CSE Dept. from beginning of Spring 2012 to end of Spring 2013. He joined the Dept. of CSE, IIT Kgp in May 2013.

Sourangshu Bhattacharya
Email: sourangshu@cse.iitkgp.ernet.in

Research Interests: *Machine learning, large scale optimization, bioinformatics, computer vision, text mining*

Sourangshu Bhattacharya is a Computer Scientist who is interested in Machine Learning and Optimization. Currently, his research focuses on Machine Learning on Big Data / Distributed Machine Learning. He has applied Machine Learning tools to various problems in Bioinformatics, Computer Vision, and Text Mining.

Prior to joining IIT Kharagpur as an Assistant Professor, he was working as a Scientist in Yahoo! Labs, Bangalore. At Yahoo!, he worked on improving the “Click Through Rate” prediction system for the “RightMedia Ad Exchange.” He also worked on learning from crowdsourced labels and learning word segmentation.

Dr. Bhattacharya did his PhD in Computer Science from the Department of Computer Science & Automation, Indian Institute of Science, Bangalore. His advisor was Dr. Chiranjib Bhattacharyya, and he was a part of the Machine Learning Lab. His PhD research areas included Bioinformatics and Machine Learning.

Dr. Bhattacharya did his M.Tech. in Computer Science from Indian Statistical Institute, Kolkata and B.Tech. in Civil Engineering from IIT Roorkee.

Sudebkumar Prasant Pal
Email: spp@cse.iitkgp.ernet.in

Research Interests: *Design and analysis of computer algorithms, computational and combinatorial geometry, graph theory and algorithms, combinatorics*

Sudebkumar Prasant Pal has research interests in the design and analysis of computer algorithms, particularly in the domains of geometry and graph/hypergraph theory. In the area of computational geometry, his contributions include results on weak visibility and convex visibility in polygons, and on the

computational and combinatorial complexity of regions visible with multiple specular and diffuse reflections. He has also worked on algorithms for channel routing, and robust high-precision algebraic and geometric computation. Later he worked on (i) combinatorial characterizations of LOCC incomparable ensembles of multipartite quantum entangled states, (ii) entanglement-assisted multiparty protocols, and (iii) purely caching based video feeds as opposed to streaming, for scalable video service by introducing the notion of virtual caching in internet proxies. In recent times, he has worked on hypergraph coding and coloring, constrained reflection paths in polygons, and applications of Lovasz' local lemma. He has held positions such as (i) Convenor, Advisory Committee for the Centre for Theoretical Studies, IIT Kharagpur, and (ii) Member Executive Council: Indian Association for Research in Computing Science. He received the Rajiv Gandhi Research Grant for Innovative Ideas in Science and Technology, 1993, from the Rajiv Gandhi Foundation and Jawaharlal Nehru Centre for Advanced Scientific Research (JNCASR), Jakkur, Bangalore. He worked as Visiting Associate Professor in the Mathematics and Computer Science department in the University of Miami, Florida, USA during the period August 1999 to May 2000.

Sudeshna Sarkar
Email: sudeshna@cse.iitkgp.ernet.in

Research Interests: *Artificial intelligence, machine learning, information retrieval, natural language processing*

Sudeshna Sarkar is a Professor in the Department of Computer Science and Engineering at Indian Institute of Technology, Kharagpur. She received the BTech degree in Computer Science & Engineering from IIT Kharagpur, India, in 1989, an MS in Computer Science from University of California, Berkeley in 1991 and Ph.D., in Computer Science & Engineering from IIT Kharagpur in 1996. She has served in the faculty of IIT Guwahati and at IIT Kanpur before joining IIT Kharagpur. Her broad research interests are in Artificial Intelligence and Machine Learning. She is currently working in the fields of natural language processing, text mining and information retrieval and content recommendation systems. She has been a principal investigator in a number of sponsored projects in these areas. Some of these are Cross language information access, Machine Translation between Indian languages, NER and POS tagging, and building of a Bengali treebank. She had been the principal scientist of Minekey, a company incubated at IIT Kharagpur and ran the research centre of Minekey at IIT Kharagpur.

Sujoy Ghose
Email: sujoy@cse.iitkgp.ernet.in

Research Interests: *Design of algorithms, artificial intelligence, and computer networks*

Sujoy Ghose received the B.Tech. degree in Electronics and Electrical Communication Engineering from the Indian Institute of Technology, Kharagpur, in 1976, the M.S. degree from Rutgers University, Piscataway, NJ, and the Ph.D. degree in computer science and engineering from the Indian Institute of Technology. He is currently a Professor in the Department of Computer Science and Engineering, Indian Institute of Technology. His research interests include design of algorithms, artificial intelligence, and computer networks.

Publications by Research Scholars (2014-2015)

Journal papers

1. Anup Kumar Bhattacharya, Sabyasachi Karati, Abhijit Das, Dipanwita Roychowdhury, Bhargav Bellur and Aravind Iyer, *Use of SIMD features to speed up eta pairing*, E-Business and Telecommunications, Communications in Computer and Information Science, Springer, Volume 455, 2014, pp 137-154, 2014.

3. Antonio A. Bruto da Costa and Pallab Dasgupta, *Formal Interpretation of Assertion-Based Features on AMS Designs*, IEEE Design & Test, vol. 32, no. 1, pp 9-17, 2014.

4. Joy Chandra Mukherjee and Arobinda Gupta, *A Review of Charge Scheduling of Electric Vehicles in Smart Grid*, IEEE Systems Journal, DOI: 10.1109/JSYST.2014.2356559

5. Joy Chandra Mukherjee, Saurabh Shukla and Arobinda Gupta, *Mobility Aware Scheduling for Imbalance Reduction through Charging Coordination of Electric Vehicles in Smart Grid*, Pervasive and Mobile Computing Journal, Elsevier, DOI: 10.1016/j.pmcj.2014.12.004

6. Kunal Banerjee, Chandan Karfa, Dipankar Sarkar and Chittaranjan Mandal. *Verification of Code Motion Techniques using Value Propagation*, IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems (TCAD), vol. 33, no. 8, 2014, pp: 1180-1193.

7. Kunal Banerjee, Dipankar Sarkar and Chittaranjan Mandal, *Extending the FSMD Framework for Validating Code Motions of Array-Handling Programs*, IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems (TCAD), vol. 33, no. 12, 2014, pp: 2015-2019.

8. Manjira Sinha and Anupam Basu, *A Study of Readability of Texts in Bangla through Machine Learning Approaches*, International Journal of Education and Information Technologies (EAIT), Springer, 2014, (Accepted).

9. Sabyasachi Karati, Abhijit Das, Dipanwita Roychowdhury, Bhargav Bellur, Debojyoti Bhattacharya and Aravind Iyer, *New algorithms for batch verification of standard ECDSA signatures*, Journal of Cryptographic Engineering, Springer, Volume 4, Issue 4, pp 237-258, 2014.

10. Sourya Bhattacharyya and Jayanta Mukherjee, *COSPEDTree: COuplet Supertree by Equivalence Partitioning of taxa set and DAG formation*, IEEE/ACM Transactions on Computational Biology and Bioinformatics, no. 1, pp. 1, PrePrints, doi:10.1109/TCBB.2014.2366778

11. Subhasish Dhal, Atanu Basu and Indranil Sen Gupta, *Managing Authentication and Detection Probability in Multi-tag RFID System*, Journal of Information Assurance and Security, 9(6), pp 316-328, November 2014.

12. Subhasish Dhal and Indranil Sen Gupta, *Object Authentication Using RFID Technology: A Multi-tag Approach*, International Journal of Computer Network and Information Security (To appear).

13. Sunny Mitra, Ritwik Mitra, Suman Kalyan Maity, Martin Riedl, Chris Biemann, Pawan Goyal and Animesh Mukherjee, *An automatic approach to identify word sense changes in text media across timescales*, Journal of Natural Language Engineering, 2015

14. Sumanta Pyne and Ajit Pal, R*untime Leakage Power Reduction using Loop Unrolling and Fine Grained Power Gating*, Journal of Low Power Electronics (JOLPE), Volume 11, Issue 1, March 2015, pp. 16-36.

15. Tanmoy Chakraborty, Suhansanu Kumar, Pawan Goyal, Niloy Ganguly and Animesh Mukherjee, *On the categorization of scientific citation profiles in computer sciences*, Communications of the ACM (CACM). (Accepted)

16. Tanmoy Chakraborty, Vihar Tammana, Niloy Ganguly and Animesh Mukherjee. *Understanding and Modeling Diverse Scientific Careers of Researchers*, Journal of Informetrics, 9:1, ISSN 1751-1577, pp. 69-78, Jan 2015.

17. Tanwi Mallick, Partha Pratim Das and Arun Kumar Majumdar, *Characterizations of Noise in Kinect Depth Images: A Review*. IEEE Sensor Journal (2014), Volume 14, Issue 6, pp. 1731-1740.

18. Tirthankar Dasgupta, Manjira Sinha, and Anupam Basu, *Computational Modelling of Morphological Effects in Bangla Visual Word Recognition*, Journal of Psycholinguistic Research (JOPR), DOI:10.1007/s10936-014-9302-x.

19. Tirthankar Dasgupta, and Anupam Basu, *Computational Models of the Lexical Representation of Bangla Compound Words in the Mental Lexicon*, Journal of Psycholinguistic Research (JOPR), Springer, 2015, (Accepted).

20. Tirthankar Dasgupta, Manjira Sinha and Anupam Basu, *Resource Creation and Development of an English-Bangla Back Transliteration System*, International Journal of Knowledge-Based and Intelligent Engineering Systems (KES), IOS Press, 2015, (Accepted).

Conference papers

1. Abhishek Chakraborty, Bodhisatwa Mazumdar, and Debdeep Mukhopadhyay, *A Practical DPA on Grain v1 using LS-SVM*, in IEEE International Symposium on Hardware Oriented Security and Trust (HOST), 2015, McLean, VA, USA.

2. Abhishek Chakraborty, Bodhisatwa Mazumdar, and Debdeep Mukhopadhyay, *Fibonacci LFSR vs. Galois LFSR: Which is More Vulnerable to Power Attacks?*, in Security, Privacy, and Applied Cryptography Engineering (SPACE), 2014, Pune, India.

3. Abhrajit Sengupta, Dhiman Saha, Shamit Ghosh, Deval Mehta, and Dipanwita Roy Chowdhury. *AEC: A practical scheme for authentication with error correction*, In Security, Privacy, and Applied Cryptography Engineering - 4th International Conference, SPACE 2014, Pune, India, October 18-22, 2014. Proceedings pages 155–170, 2014.

4. A. De, S. Bhattacharya, P. Bhattacharya, N. Ganguly, and S. Chakrabarti, *Learning a Linear Influence Model from Transient Opinion Dynamics*, in CIKM 2014.

5. Ajay Kant Singh, Subhasish Dhal and Indranil Sen Gupta, *An Approach to Solve Tracking and Message Blocking Problems in RFID*, in Proceedings of the 3rd International Conference on Communications System and Network Technology (CSNT 2014), pp 1187-1191, April 2014.

6. Anju P. Johnson, Sayandeep Saha, Rajat Subhra Chakraborty, Debdeep Mukhopadhyay and Sezer Goren, *Fault Attack on AES via Hardware Trojan Insertion by Dynamic Partial Reconfiguration of FPGA over Ethernet*,Workshop on Embedded Systems Security (WESS, part of ACM ESWEEK) 2014, New Delhi, India.

7. Debapriya Basu Roy, Debdeep Mukhopadhyay, Masami Izumi and Junko Takahashi, *Tile Before Multiplication: An Efficient Strategy to Optimize DSP Multiplier for Accelerating Prime Field ECC for NIST Curves*, DAC 2014: 1-6.

8. Dhiman Saha and Dipanwita Roy Chowdhury, *Diagonal Fault Analysis of Grøstl in Dedicated MAC Mode*, To appear in 8th IEEE International Symposium on Hardware-Oriented Security and Trust, HOST 2015, May 5-7, 2015, McLean, Virginia, USA.

9. Dhiman Saha, Sukhendu Kuila and Dipanwita Roy Chowdhury, *EscApe : Diagonal Fault Analysis of APE*, In Proceedings of the 15th International Conference on Cryptology in India, INDOCRYPT 2014, December 14-17, 2014, New Delhi, India.

10. Dhiman Saha, Sukhendu Kuila and Dipanwita Roy Chowdhury, *Misusing Misuse-Resistance in APE*, Accepted at Directions in Authenticated Ciphers - DIAC 2014 , August 23-24, 2014, Santa Barbara, USA.

11. Durga Prasad Sahoo, Debdeep Mukhopadhyay, and Rajat Subhra Chakraborty, *Design of Low Area-overhead Ring Oscillator PUF with Large Challenge Space*, in Proceedings of the International Conference on Reconfigurable Computing and FPGAs (ReConFig), pp. 1-6, December 2013, Cancun, Mexico.

12. Durga Prasad Sahoo, Debdeep Mukhopadhyay, and Rajat Subhra Chakraborty, *Formal Design of Composite Physically Unclonable Function*, in Proceedings of the Workshop on Security Proofs for Embedded Systems (PROOFS), September 2013, Santa Barbara, California, USA.

13. Durga Prasad Sahoo, Sayandeep Saha, Debdeep Mukhopadhyay, Rajat Subhra Chakraborty, and Hitesh Kapoor, *Composite PUF: A New Design Paradigm for Physically Unclonable Functions on FPGA*, in Proceedings of the IEEE International Symposium on Hardware-Oriented Security and Trust (HOST), May 2014, Arlington, VA, USA.

14. Jimmy Jose, Sourav Das and Dipanwita Roy Choudhury, *Inapplicability of Fault Attacks against Trivium on a Cellular Automata Based Stream Cipher,* ACRI 2014, LNCS vol. 8751, pp. 427-436, Springer 2014.

15. Joy Chandra Mukherjee and Arobinda Gupta, *Mobility Aware Event Dissemination in VANET*, 16th International Conference on Distributed Computing and Networks (ICDCN), Goa, India.

16. Joy Chandra Mukherjee, Saurabh Agarwal and Arobinda Gupta, *Distributed Event Notification in VANET with Multiple Service Providers*, 8th ACM International Conference on Distributed Event-Based Systems (DEBS), Mumbai, India, 2014: 334-337.

17. K. K. Sharma, Kunal Banerjee and Chittaranjan Mandal, *A Scheme for Automated Evaluation of Programming Assignments using FSMD based Equivalence Checking,* IBM Collaborative Academia Research Exchange (I-CARE), October 2014, pp: 10:1-10:4.

18. K. K. Sharma, Kunal Banerjee, Indra Vikas and Chittaranjan Mandal, *Automated Checking of the Violation of Precedence of Conditions in else-if Constructs in Students' Programs*. International Conference on MOOC, Innovation and Technology in Education (MITE), December 2014, pp: 201-204.

19. Koustav Rudra, Abhijnan Chakraborty, Manav Sethi, Shreyasi Das, Niloy Ganguly, and Saptarshi Ghosh, *#FewThingsAboutIdioms: Understanding Idioms and its Users in the Twitter Online Social Network*, to appear in Proceedings of the 19th Pacific-Asia Conference on Knowledge Discovery and Data Mining (PAKDD), Ho Chi Minh City, Vietnam, May 2015.

20. Kunal Banerjee, *An Equivalence Checking Mechanism for Handling Recurrences in Array-Intensive Programs*, ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages (POPL): Student Research Competition, January 2015.

21. Kunal Banerjee, Chittaranjan Mandal and Dipankar Sarkar, *Deriving Bisimulation Relations from Path Extension Based Equivalence Checkers*. IMPECS-POPL Workshop on Emerging

Research and Development Trends in Programming Languages (WEPL), January 2015.

22. Kunal Banerjee, Chittaranjan Mandal and Dipankar Sarkar, *Extending the Scope of Translation Validation by Augmenting Path Based Equivalence Checkers with SMT Solvers*, International Symposium on VLSI Design and Test (VDAT), July 2014, pp: 1-6.

23. Manjira Sinha, Tirthankar Dasgupta, and Anupam Basu, *Design and Development of an Online Computational Framework to Facilitate Language Comprehension Research on Indian Languages*, 9th International Conference on Language Resources and Evaluation (LREC), 2014,pp: 203-210, Iceland.

24. Manjira Sinha, Tirthankar Dasgupta, Surabhi Agrawal, Sneha Jain, Nidhi Bagaria, and Anupam Basu, *Development of Entertainment and Social Interaction Applications to improve Quality-of-Life(QOL) of people with cerebral palsy*, IEEE Technological symposium 2014 , TechSym'14, pp:19-24.

25. Manjira Sinha, Tirthankar Dasgupta, and Anupam Basu, *Inuence of Target Reader Background and Text Features on Text Readability in Bangla: A Computational Approach*, 25th International Conference on Computational Linguistics (COLING), 2014, pp: 345-354, Dublin, Ireland.

26. Manjira Sinha,Tirthankar Dasgupta, Anupam Basu, *Text Readability in Hindi: A Comparative Study of Feature Performances Using Support Vectors*, International Conference on Natural Language Processing (ICON), 2014, Goa, India, (Accepted).

27. Moumita Saha, *A Graph Based Approach to Multi-view Clustering*, 5th International Conference on Pattern Recognition and Machine Intelligence (PReMI 2013), pp. 128-133, 2013.

28. Moumita Saha and Pabitra Mitra. *VLGAAC: Variable Length Genetic Algorithm Based Alternative Clustering*, 21st International Conference on Neural Information Processing (ICONIP 2014), pp. 194-202, 2014.

29. P. Bhattacharya, M. B. Zafar, N. Ganguly, S. Ghosh, and K. P. Gummadi, I*nferring User Interests in the Twitter Social Network*, ACM Recommender System Conference (RecSys), Silicon Valley, California, USA, 2014.

30. P. Bhattacharya, S. Ghosh, J. Kulshrestha, M. Mondal, M. B. Zafar, N. Ganguly, and K. P. Gummadi, *Deep Twitter Diving: Exploring Topical Groups in Microblogs at Scale*, ACM Computer Supported Cooperative Work and Social Computing (CSCW), Baltimore, MD, USA, Feburary 2014

31. Partha De, Kunal Banerjee and Chittaranjan Mandal, *A BDD based Secure Hardware Design Method to Guard Against Power Analysis Attacks*, International Symposium on VLSI Design and Test (VDAT), July 2014, pp: 1-2.

32. Partha De, Kunal Banerjee, Chittaranjan Mandal, Debdeep Mukhopadhyay, *Circuits and Synthesis Mechanism for Hardware Design to Counter Power Analysis Attacks*, Euromicro Conference on Digital System Design (DSD), August 2014, pp: 520-527.

33. Phuong Ha Nguyen, Durga Prasad Sahoo, Debdeep Mukhopadhyay and Rajat Subhra Chakraborty, *Cryptanalysis of Compsite PUFs* (invited paper), in International Symposium on VLSI Design and Test (VDAT), July 2014, Coimbatore, India.

34. Phuong Ha Nguyen, Durga Prasad Sahoo, *Lightweight and Secure PUFs: a survey* (invited paper), inInternational Conference on Security, Privacy and Applied Cryptographic Engineering (SPACE), October, 2014, Pune, India.

35. Phuong Ha Nguyen, Durga Prasad Sahoo, Rajat Subhra Chakraborty and Debdeep Mukhopadhyay, *Cryptanalysis of Robust Ring Oscillator PUF with Enhanced Challenge-Response Set*, in Design, Automation and Test in Europe (DATE), March 2015, Grenoble, France.

36. Prakash Dey, Abhishek Chakraborty, Avishek Adhikari, and Debdeep Mukhopadhyay, *Improved Practical Differential Fault Analysis of Grain-128*, in Design, Automation and Test in Europe (DATE), 2015, Grenoble, France.

37. Rajorshee Raha, Aritra Hazra, Akash Mondal, Soumyajit Dey, Partha Pratim Chakrabarti and Pallab Dasgupta, *Synthesis of Sampling Modes for Adaptive Control*, Accepted for Publication in 4th IEEE International Conference on Control System, Computing and Engineering (ICCSCE), November 2014

38. Ranita Biswas and Partha Bhowmick, *On Finding Spherical Geodesic Paths and Circles in ℤ3*, 18th IAPR International Conference on Discrete Geometry for Computer Imagery: DGCI'14, 10-12 Sep 2014, Siena, Italy, LNCS 8668, pp. 396-409.

39. Sabyasachi Karati and Abhijit Das, *Faster batch verification of standard ECDSA signatures using summation polynomials*, 12th International Conference on Applied Cryptography and Network Security (ACNS 2014), Lecture Notes in Computer Science #8479, pp 438-456, Jun 10-13, 2014, Lausanne, Switzerland.

40. Sabyasachi Karati, Abhijit Das and Dipanwita Roychoudhury, *Randomized batch verification of standard ECDSA signatures*, Fourth International Conference on Security, Privacy, and Applied Cryptography Engineering (SPACE 2014), Lecture Notes in Computer Science #8804, pp 237-255, Oct 18-22, 2014, Pune, India.

41. Sabyasachi Karati and Abhijit Das, *Batch verification of EdDSA signatures*, Fourth International Conference on Security, Privacy, and Applied Cryptography Engineering (SPACE 2014), Lecture Notes in Computer Science #8804, pp 256-271, Oct 18-22, 2014, Pune, India.

42. Saurav Kumar Ghosh, Aritra Hazra and Soumyajit Dey, *RELSPEC: A Framework for Early Reliability Refinement of Embedded Applications*, Accepted for Publication in 28th IEEE International Conference on VLSI Design (VLSID), January 2015.

43. Sikhar Patranabis, Abhishek Chakraborty, P. Nguyen Ha, and Debdeep Mukhopadhyay, *A Biased Fault Attack on the Time Redundancy Countermeasure for AES*, in Constructive Side-Channel Analysis and Secure Design (COSADE), 2015, Berlin, Germany.

44. Shamit Ghosh, *CASca:A CA Based Scalable Stream Cipher*, In International Conference on Mathematics and Computing, 2015

45. Shamit Ghosh, Abhrajit Sengupta, Dhiman Saha, and Dipanwita Roy Chowdhury, *A scalable method for constructing non-linear cellular automata with period 2^n- 1*, In Cellular Automata - 11th International Conference on Cellular Automata for Research and Industry, ACRI 2014, Krakow, Poland, September 22-25, 2014. Proceedings, pages 65–74, 2014.

46. Shamit Ghosh and Dipanwita Roy Chowdhury, *Preventing Fault Attack on Stream Cipher using Randomization*, in IEEE Int. Symposium on Hardware-Oriented Security and Trust (HOST), 2015

47. Shashank Sharma, Sourya Bhattacharyya, Arunava Biswas, Jayanta Mukherjee, Parimal Kumar Purkait, and Alok Kanti Deb, *Automated detection of newborn sleep apnea using video monitoring system*, 8th International Conference on Advances in Pattern Recognition (ICAPR), Indian Statistical Institute (ISI), Kolkata, India, January 4-7, 2015.

48. Soumajit Pramanik, Pranay Hasan Yerra and Bivas Mitra, *"Whom-to-Interact: Does Conference Networking Boost Your Citation Count?"*, 2nd IKDD Conference on Data Sciences(CoDS), Bangalore, India, March 18-21, 2015. (Accepted)

49. Soumyadip Bandyopadhyay, *Behavioural Verification of Petri net based Models of Programs,* (POPL-2015) (SRC)

50. Soumyadip Bandyopadhyay, Dipankar Sarkar and Chittaranjan Mandal,*Translation Validation using Path-Based Equivalence Checking of Petri net based Models of Programs*, WEPL (co-located with POPL-2015)

51. Soumyadip Bandyopadhyay, Dipankar sarkar, Chittaranjan Mandal, *An Efficient Equivalence Checking Method for Petri net based Models of Programs*, 37th International conference on Software engineering (ICSE-2015) (accepted)

52. S. K. Dandapat, S. Pradhan, B. Mitra, R. Roychoudhury, and N. Ganguly, *ActivPass: Your Activity is Your Password, Accepted in CHI, 2015*, Seol, South Korea.

53. Sourya Bhattacharyya and Jayanta Mukhopadhyay, *COuplet Supertree by Equivalence Partitioning of taxa set and DAG formation*, Proceedings of the 5th ACM Conference on Bioinformatics, Computational Biology and Health Informatics (ACM-BCB), Newport, California, September 2014, pp. 259-268

54. Subhasish Dhal and Indranil Sen Gupta, *A New Authentication Protocol for RFID communication in Multi-tag Arrangement*, in Proceedings of the 8th International Conference on Computing for Sustainable Global Development (INDIACom 2014), pp 668-673, March 2014.

55. Subhasish Dhal and Indranil Sen Gupta, *Protocol to Authenticate the Objects Attached with Multiple RFID tags*, in Proceedings of Emerging Trends in Computing and Communication (ETCC 2014), pp 149-156. March 2014.

56. Sukhendu Kuila, Dhiman Saha, Madhumangal Pal and Dipanwita Roy Chowdhury, *CASH – Cellular Automata based Parameterized Hash*, In Proceedings of 4th International Conference on Security, Privacy and Applied Cryptographic Engineering - SPACE 2014, October 18-22, 2014, Pune, India.

57. Sukhendu Kuila, Dhiman Saha, Madhumangal Pal and Dipanwita Roy Chowdhury, *Practical Distinguishers Against 6-Round Keccak-f Exploiting Self-Symmetry,* In Proceedings of the 7th International Conference on Cryptology, AFRICACRYPT 2014, Marrakesh, Morocco, May 28-30, 2014, pp. 88-108

58. Suman Kalyan Maity, T.Venkata Manoj, and Animesh Mukherjee, *Opinion dynamics in correlated time-varying social networks*, in proceedings of the 2014 ASE International Conference on Social Computing (SocialCom '14), Stanford, CA, USA, May 27 - 31, 2014

59. Sumanta Pyne and Ajit Pal, *Loop Unrolling with Fine Grained Power Gating for Runtime Leakage Power Reduction*, in the proceedings of 18th International Symposium on VLSI Design and Test (VDAT 2014), July 16-18, 2014, Coimbatore, India.

60. S. Pradhan, S. K. Dandapat, N. Ganguly, B. Mitra and P. De, *Aggregating Inter-App Traffic to Optimize Cellular Radio Energy Consumption on Smartphones, Comsnet 2015*, Bangalore, India.

61. Tanmoy Chakraborty, Natwar Modani, Ramasuri Narayanam and Seema Nagar, *DiSCern: A Diversified Citation Recommendation System for Scientific Queries*, In 31st IEEE International Conference on Data Engineering (ICDE), Seoul, Korea, April 13-17, 2015. (Accepted)

62. Tanmoy Chakraborty, Niloy Ganguly and Animesh Mukherjee, *Automatic Classification of Scientific Groups as Productive: An Approach based on Motif Analysis*, In Proceedings of IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM), Beijing, China August 17-20, 2014, pp. 130-137.

63. Tanmoy Chakraborty, Sriram Srinivasan, Niloy Ganguly, Animesh Mukherjee and Sanjukta Bhowmick, *On the permanence of vertices in network communities*, In Proceedings of 20th ACM SIGKDD Conference on Knowledge Discovery and Data Mining, New York City, August 24 - 27, 2014, pp. 1396-1405.

64. Tanmoy Chakraborty, Suhansanu Kumar, Pawan Goyal, Niloy Ganguly and Animesh Mukherjee, *Towards a Stratified Learning Approach to Predict Future Citation Counts*, In Proceedings of ACM/IEEE Digital Libraries (jointly with JCDL and TPDL), London, United Kingdom, September 8-12, 2014, pp. 351-360.

65. Tanmoy Chakraborty, Vihar Tammana, Niloy Ganguly and Animesh Mukherjee, *Analysis and Modeling of Lowest Unique Bid Auctions*, In Proceedings of Sixth ASE International Conference on Social Computing (SocialCom-2014), Stanford, CA, USA, May 27 - May 31, 2014.

66. Tanwi Mallick, Partha Pratim Das and Arun Kumar Majumdar, *Estimation of the orientation and distance of a mirror from kinect depth data,* In Computer Vision, Pattern Recognition, Image Processing and Graphics (NCVPRIPG 2013), Proc. 4th National Conference on (2013), pp. 1-4.
67. Tanwi Mallick, Partha Pratim Das and Arun Kumar Majumdar, *Study of interference noise in multi-kinect set-up,* In Computer Vision Theory and Applications (VISAPP 2014), Proc. 9th International Conference on (2014), pp. 173-178.

68. Tanwi Mallick, Rishabh Agrawal, Partha Pratim Das and Arun Kumar Majumdar, *Omnidirectional, Reconstruction of Human Figures from Depth Data using Mirrors,* In Computer, Vision Theory and Applications (VISAPP 2015), 10th International Conference on (2015), Accepted.

69. Tapas Mishra and Sudebkumar Prasant Pal, *Bicoloring covers for graphs and hypergraphs,* arXiv preprint arXiv:1501.00343, 2015.

70. Tirthankar Dasgupta, Manjira Sinha and Anupam Basu, *Development of Accessible Toolset to Enhance Socia Interaction Opportunities for People with Cerebral Palsy in India*, 16th International ACM SIGACCESS Conference on Computers and Accessibility (ASSETS), 2014, pp:249-250, Rochester, New York.

71. Tirthankar Dasgupta, Manjira Sinha and Anupam Basu, *Web Browsing Interface for People with Sever Speech and Motor Impairment in India*, 16th International ACM SIGACCESS Conference on Computers and Accessibility (ASSETS), 2014, pp:285-286, Rochester, New York.

72. T. Swarnkar, S. N. Sim˜oes, D. C. Martins-JR, A. Anura, H. Brentani, R. F. Hashimoto and P. Mitra, *Multiview clustering on PPI network for gene selection and enrichment from microarray data*. In 2014 IEEE 14th International Conference on Bioinformatics and Bioengineering, Boca Raton, Florida, USA, IEEE.

Awards and Achievements (2013 – 2014)

1. **Chandan Karfa:** *Innovative Student Projects Award 2013 (Doctoral Level)*, for his PhD Thesis "Formal Verification of Behavioural Transformations During Embedded System Design," from Indian National Academy of Engineering (INAE).

2. **Chandan Karfa:** *TechnoInventor Award 2013*, for his PhD Thesis "Formal Verification of Behavioural Transformations During Embedded System Design," from India Electronics and Semiconductor Association (IESA).

3. **Kunal Banerjee:** *Best Paper Award*, for the paper "Experimentation with SMT Solvers and Theorem Provers for Verification of Loop and Arithmetic Transformations" presented at the conference "IBM Collaborative Academia Research Exchange (I-CARE), 2013."

4. **Parantapa Bhattacharya and Saptarshi Ghosh:** *First Prize*, for their joint poster in Microsoft Techvista 2013.

5. **Tanmoy Chakraborty:** *Best Presentation Award*, for his paper in "Workshop on Science and Engineering of Social Networks (SCINSE), 6th International Conference on Communication System and Networks (COMSNETS-2014)."

Research Scholars who Graduated in 2014-2015

PhD Students

Bibhas Ghoshal
Kallol Mallick
Prasenjit Mondal
Rishiraj Saha Roy
Sabyasachi Karati
Sanjay Chatterji
Sudip Roy
Subhadip Kundu
Tapas Samanta

Bodhisatwa Mazumdar
Maunendra Sankar De Sarkar
Rajib Ranjan Maiti
Ruchira Naskar
Sandip Karmakar
Satya Gautam Vadlamudi
Soma Saha
Sudipta Saha

MS Students

Arnab Dhar
Binanda Sengupta
Partha De
Souvik Kolay
Swadhin Pradhan

Ayan Palchaudhuri
Parnab Kr. Chanda
Suvadeep Hajra
Srinivas Virinchi