# Research Scholars' Day


## Department of Computer Science and Engineering

IIT Kharagpur

March 20 2016

# Department of Computer Science and Engineering

**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 20th day of March, 2016. This event gives the research students a unique opportunity to present their work, share research ideas, get feedback and also helps the faculty members to get an appraisal of the complete picture of the research activities carried out by the research scholars in the department. The day also provides the research scholars with a platform to demonstrate their cultural aptitude. Like the previous years, I am sure that 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***

# PhD Scholars

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

***Supervisor: Dr. Pralay Mitra***

*Abantika is a PhD Scholar at IIT Kharagpur in Computer Science and Engineering Department. Her PhD work is supervised by Dr. Pralay Mitra. Her research interests mainly include Bioinformatics and Computational biology. She is currently working on the problem of Protein Interactor Discovery. She has received M.E. degree from the Department of Computer Science Engineering, Jadavpur University and received a B.Tech. degree from Academy of Technology. She has one year of teaching experience as teaching assistant in Computer Science Engineering Department, Jadavpur University. She has worked in Cognizant Technology Solutions as Programmer Analyst Trainee in .Net Technology. She has also worked in Tata Consultancy Services as Assistant System Engineer Trainee in Java Technology.*

## Protein Interactor Discovery

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.

**Abhijit Mondal**
Email: abhimondal@iitkgp.ac.in
Joined the department in: September 2015

***Supervisor: Dr. Sandip Chakraborty***

*Abhijit Mondal received B.tech. degree in Computer Science & Engineering from Kalyani Govt. Engg. College in 2010. He joined Department of Computer Science and Engineering of Indian Institute of Technology Guwahati in 2010 and received M.Tech degree in July, 2012. From October 2012 to July 2015, He worked as Member of Technical Staff in Veveo India Pvt. Limited. He joined research program in Deportment of Computer Science & Engineering of Indian Institue of Techonology Kharagpur in July 2015. Since then he have interest in Wireless Network.*

## Improve User Experience with High Speed Wireless Backbone

The next generation Internet architecture is gradually shifting from fixed communication layouts to mobile and dynamic communication entities, along with a coherent change in application traffic pattern. In line of this, the design, development and planning for future “connected cities” demand high speed wireless backbone networks for community usage as well as for metropolitan area communications, so that extensive supports for seamless mobility across the network become prominent. Although the designs of high speed communication and Gigabit wireless technologies are in pace, recent studies shown that there are significant coordination gaps among the lower layer high speed communication technologies and the upper layer protocol principles. This leads to a non-optimal usage of communication resources, like bandwidth and network capacity, and significantly affects end-user experience. The objective of this project is to design, develop and implement a high speed wireless access network that supports network resilience and better end-user experience in terms of quality-of-service (QoS) and quality-of-experience (QoE). In this project, our first objective is

to develop a prototype testbed for high speed wireless access along with a controllable software defined radio (SDR) platform, and then analyze the effect of physical (PHY) and medium access control (MAC) parameter settings over the upper layer protocol performance. This analysis is non-trivial and significantly differs from the existing studies because of the emerging traffic behaviors at the next generation dense access networks. Based on this analysis, we aim to design a set of coordination protocols at MAC and transport layers, with a special focus on end-to-end semantics for network resilience and application layer QoS. Finally, we aim to implement the advanced protocols over the testbed, and analyze their performance in real network scenarios.

**Abhijnan Chakraborty**
Email: abhimondal@iitkgp.ac.in
Joined the department in: July 2014

***Supervisor: Prof. Niloy Ganguly***

*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 in 2014. He has been awarded Prime Minister's Fellowship for Doctoral Research in 2015. 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, ICWSM, and Hypertext etc.*

**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 honor individual users sampling strategies, yet maximize coverage over information with "long-term importance" and minimize the delay in getting such information.

**Abhik Jana**
Email: abhikjana1@gmail.com
Joined the department in: January 2015

***Supervisor: Dr. Pawan Goyal***

*I am a Ph.D. student in the Department of Computer Science and Engineering, IIT Kharagpur, since Jan 2015. My supervisor is Dr. Pawan Goyal. My basic interest lies in the study of Natural Language Processing, Cognitive Computing.*

**Enriching Wikipedia pages from authoritative sources for enhanced entity linking**

Wikipedia (introduced in 2001) is an online encyclopedia that has evolved as the largest repository of collaboratively curated encyclopedic knowledge having millions of articles, in more than 200 languages. Although initially it was not created with the aim of helping studies in natural language processing, its ever-growing size, wide coverage, and high quality provides an appealing research opportunity. Its coherent structure opens up the space for leveraging those tasks whose performance is thought to benefit from lexical semantic knowledge like word sense disambiguation, named entity categorization, entity linking etc. It is also believed by the researchers that the structure of Wikipedia naturally encodes the semantic relationships in a language similar to human cognition since it was spontaneously developed by a mass. Despite of being such a reliable knowledge base, previous studies have shown that there is a lack of important facts in trunk and long-tail entity pages, even in the presence of relevant sources which raises two major problems:

a) Insufficient facts in Wikipedia which lead to incomplete knowledge representation for entities.
b) Insufficient entity representation leading to sub-optimal performance of entity linking tasks due to lack of sufficient context information.

In my Ph.D thesis, broadly I would be answering the following two interesting questions:

1) How can we automatically enrich Wikipedia pages from authoritative sources like scholarly and scientific articles?
2) How can we improve entity linking for such concepts in the absence of sufficient contextual 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)***

**Link Prediction in Social network**

In link prediction (LP), a graph mining algorithm is presented as a graph, and has to rank, for each node, other nodes that are candidates for new linkage. LP is strongly motivated by social search and recommendation applications. LP techniques often focus on global properties (graph conductance,

hitting or commute times, Katz score) or local properties (Adamic-Adar and many variations, or node feature vectors), but rarely combine these signals. Furthermore, neither of these extremes exploit link densities at the intermediate level of communities. We attempt to describe a discriminative LP algorithm that exploits two new signals. First, a co-clustering algorithm provides community level link density estimates, which are used to qualify observed links with a surprise value. Second, links in the immediate neighborhood of the link to be predicted are not interpreted at face value, but through a local model of node feature similarities. The resulting predictor is simple and efficient. In our work we try to evaluate the new predictor using five diverse data sets that are standard in the literature.

**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



**Amit V. Nandedkar**
Email: nandedkar_amit@yahoo.com
Joined the department in: September 2013


***Supervisor: Prof. Jayanta Mukhopadhyay, Prof. Shamik Sural***

Amit V. Nandedkar received his B.E. (Computer Science & Engg.) degree in 2001 and M.E. (EC specialization in Computer Technology) degree in 2004 from S.R.T.M. University, Nanded, (M.S.). He joined the SGGS Institute of Engg. & Technology, Nanded as a lecturer in June 2004. Since July 2013 he has been a QIP research scholar in the school of Information Technology.

**Document Image Processing & Retrieval**

The primary objective of this research work is to develop novel algorithms for document image retrieval and evaluating their performance. The task also includes development of various preprocessing and segmentation techniques for document images, e.g. separation of text and graphics, detection of stamps, logos, and signatures.


**Amrith Krishna**
Email: amrith@iitkgp.ac.in
Joined the department in: September 2015


***Supervisor: Prof. Pawan Goyal***

**Sanskrit Computational Linguistics**

The bulk of the Sanskrit literature is written in the form of poetry (Shloka), primarily owing to the traditional use of free word order enriched with various metrical patterns in sentence constructions. However, the peculiarities of such constructs render the state-of-the-art NLP techniques often inept at the task and a full-fledged parser is required to handle the shlokas. Similarly, In Sanskrit texts, it is common to find challenges due to rich inflectional morphology, phonetic sound joins across word boundaries (Sandhi) etc. My research problem currently revolves around building tools that can handle syntactic constructs in Sanskrit.

**Anandarup Mukherjee**
Email: arm@sit.iitkgp.ernet.in
Joined the department in: December 2014

***Supervisor: Dr. Sudip Misra***

*Anandarup Mukherjee is currently pursuing PhD in Engineering, from Indian Institute of Technology, Kharagpur (IIT Kharagpur). His current designation is Senior Research Fellow (SRF) and he is engaged with both the departments of Computer Science and Engineering as well as Agriculture and Food Engineering (AgFE) at IIT Kharagpur. He volunteers as a part of the Membership development team at the IEEE Student branch at IIT Kharagpur. He finished his M.Tech and B.Tech from West Bengal University of Technology in the years 2012 and 2010, respectively. He has served as an Assistant professor in the department of Electronics & Communication Engineering at University of Engineering & Management, Jaipur (2012-2014); prior to that he served as a lecturer in the department of Information technology at Institute of Engineering & Management, Kolkata (2011-2012).*

## Networked Robots

The various challenges faced during development of a networked robot-centric architecture are being addressed. The robots range from basic ground-based rovers to micro and macro aerial rovers and platforms. These robots are controlled over the network.

**Anirban Santara**
Email: anirban_santara@iitkgp.ac.in
Joined the department in: September 2015

***Supervisor: Dr. Pabitra Mitra***

*Anirban graduated from the Department of Electronics and Electrical Engineering, IIT Kharagpur in 2015 and joined Direct PhD program in the Department of Computer Science and Engineering, IIT Kharagpur. His prime area of focus is Machine learning with Artificial Neural Networks (Deep Learning). Currently he designs task-specific deep learning architectures and learning algorithms for a number of applications like image understanding, speech recognition, natural language understanding, and medical image analysis, remote sensing and climate data-mining. He is the coordinator of the reading sessions of the newly formed Deep Learning Research Group.*

## Multi-modal Deep Learning

Search for a vector space where every point represents a concept along with its physical (visual), spoken and textual descriptions.

**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. Hardware Trojan Horses (HTH) 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 emerges 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 applications which provide real-time computational capabilities. If the FPGA is remotely accessed over a regular Ethernet connection, some arbitrary modifications on the existing dynamically reconfigurable FPGA 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 designed 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, are practically impossible. Non-invasive detection methods utilizing side-channel analysis can be used to detect the presence of hardware Trojan horses. A restrictive mode of DPR can be implemented that can prove effective in preventing Trojan insertion, at the cost of 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 applications, as accelerated methods can speed the encryption and decryption on FPGAs. So ability to protect the FPGAs from hardware Trojans is very important. This motivates us to study countermeasures against hardware Trojan attacks on FPGA based systems and to develop a Hardware Trojan Evaluation Platform on FPGAs.

**Anupam Mandal**
Email: amandal@cse.iitkgp.ernet.in, anupam_405@yahoo.com
Joined the department in: December 2011

***Anupam Mandal*** *received his B.E. and M.S. degree in Computer Science and Engineering from National Institute of Technology, Durgapur and Indian Institute of Technology, Madras respectively. He is currently a scientist at Center for Artificial Intelligence and Robotics, Bangalore. Since December 2011, he has joined the department of Computer Science & Engineering in IIT Kharagpur as a sponsored research scholar. His research interests are in the area of speech recognition and VoIP technologies.*

***Supervisor: Prof. Pabitra Mitra***

**Keyword spotting in speech**

My current work is on spotting keywords in continuous speech, a sub-area of continuous speech recognition. I am focusing on template-based approaches to keyword spotting that require lesser training data and may perform robustly in presence of noise and channel based degradations. As these methods involve matching of sound instances present in an utterance without any prior assumption of the underlying language, they may also work well for multilingual speech. My research is targeted towards novel methods of speech template representation and matching.

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

***Supervisor: Prof. Sudeshna Sarkar***

*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 Natural Language Processing and Machine Learning.*

**Natural Language Processing in Indian Languages using Deep Learning**

One of the main challenges in developing NLP systems for Indian languages is the lack of sufficient annotated data for training the systems. Besides, the morphological richness of many of the Indian languages makes the problem even more challenging. For example, machine translation systems require parallel corpora and parsers require parsed annotated sentences for training.

Deep learning frameworks such as deep neural networks (DNN), recurrent neural networks (RNN), convolutional neural networks (CNN) and recursive neural networks have been successfully used in NLP
tasks. Some of the deep learning based NLP systems have surpassed the traditional systems in terms of performance. Given the promising performance of the DL systems in NLP, are to exploring different DL methods for machine translation and parsing of Indian languages. We primarily focus on Hindi, Bengali and English languages. We have explored some encoder-decoder based deep learning architectures for machine translation and attention-based model for machine translation on the above mentioned language pairs. We will be working on methods to improve the quality of the translation

when the size of the available parallel corpus is small.

In parsing we are trying to develop a good quality Bengali parser. But annotated Bengali treebank is extremely limited in size. We are exploring for methods for cross-lingual parsing where the parser for a resource rich language can be used for developing a good quality parser for a resource poor language. We are also looking into methods like delexicalization etc. for improving the parsers for low resource languages.

**Ayan Kumar Bhowmik**
Email: ayankumarbhowmick@gmail.com
Joined the department in: September 2015

***Supervisor: Prof. Bivas Mitra***

*Ayan Kumar Bhowmik obtained his B.Tech in Computer Science and Engineering from St. Thomas College of Engineering and Technology under West Bengal University of Technology in 2011. Then he briefly worked as a Programmer Analyst in Cognizant Technology Solutions India Pvt. Ltd from August, 2011 to September, 2012. Then he obtained my M.E. in Computer Science and Engineering from IIEST Shibpur (formerly known as Bengal Engineering and Science University, Shibpur) in 2015. He joined IIT Kharagpur as a PhD scholar in the September, 2015.*

**Analyzing the impact of Information Propagation in Online Social Networks**

My broad area of research is focused on the problem of information propagation and its impact on different social networks. The major objective is to explore the role of information propagation in Twitter and Location-based social networks (LBSNs) like Yelp. In case of Twitter, it leads to the formation of information cascade of retweet activities for some tweets contributing to their widespread popularity. In case of LBSN, spread of information about businesses leads to new customers visiting the business thus leading to its popularity. Using this knowledge, we can recommend candidate locations for starting up new businesses so as to maximize its popularity.

**Ayan Mondal**
Email: mondalayan12@gmail.com
Joined the department in: Jan 2015

***Supervisor: Dr. Sudip Misra***

*Ayan Mondal is presently pursuing his Doctor of Philosophy (Ph.D.) degree from the Department of Computer Science and Engineering, Indian Institute of Technology Kharagpur, India. His current research interests include algorithm design for Smart Grid, Wireless Sensor Networks and Big Data Networking. He received his Master of Science (by Research) (M.S.) degree from the School of Information Technology, Indian Institute of Technology Kharagpur, India in 2015. His M.S. Thesis is entitled as "Distributed Energy Management in Smart Grid". He received his Bachelor of Technology degree in Electronics and Communication Engineering from St. Thomas' College of Engineering and Technology, West Bengal University of Technology, India in 2012. He is a graduate student member of IEEE and ACM.*

**Task Management in MapReduce for Big Data Networks**

Big Data Network (BDN) is one of the important issues which is drawing attention of many researchers. BDN can handlw large-scale datasets created in each second over the World. Therefore, we plan to design different schemes for Map and Reduce Tasks scheduling, inter- and intra-data center networks, and Edge networks for handling massive generated data while analyzing performance of the existing scheduling approach used for distributed file systems.

**Bidisha Samanta**
Email: bidisha.samanta@gmail.com
Joined the department in January 2016

*Bidisha Samanta received her Master's degree in Computer Science and Engineering from Indian Institute of Technology Kharagpur, in 2013. She has completed her Bachelors in the same discipline from Heritage Institute of Technology, under West Bengal University of Technology, 2011. After her postgraduation she worked with Yahoo! India for one and half years then in Amazon for another one year. She has been a research scholar at the department of computer science and engineering since January 2016*

***Supervisor: Prof. Niloy Ganguly***

**Rank tweets based on future popularity**

It is an interesting problem related to dynamically evolving social network to study the popularity dynamics of an item in microblogging sites like Twitter. It is extremely important to predict the popularity of a tweet and rank them based on the tendency of gaining attention. For instance, Sachin Tendulkar's tweet "Angry Disappointed and Frustrated.. #BAdserviceBA Family member's Waitlisted ticket not confirmed despite seats being available" on British Airways went viral, and it had a negative impact on the authorized organization.

**Bijju Kranthi Veduruparthi**
Email: bijjukranthi@cse.iitkgp.ernet.in
Joined the department in June 2013

***Bijju Kranti Veduruparthi*** *has been a PhD student in the Department of Computer Science and Engineering, IIT Kharagpur, since July 2013. His research interests are in the areas of Computer Vision, Medical Image Processing and Pattern Recognition*

***Supervisors: Prof. Jayanta Mukhopadhyay, Prof. Partha Pratim Das***

**Growth & decay modeling for prognosis of lung cancer patients under radio-therapeutic treatment**

Lung Tumor Volume estimation on imaging modalities is required to assess the extent of the tumor for diagnosis. Adaptive Radiation Therapy(ART) aims at using serial on treatment ConeBeam Computer Tomography(CBCT) scans for accurate estimation of the Planning Target Volume(PTV) after taking patient movement, tumor growth, deformations with respect to organs into account. Our work aims at minimizing the PTV to allow radiologists to give more focused radiation treatment thereby reducing the chance of tumor regrowth and also reducing side effects of radiation. We want to build novel techniques for understanding tumor growth, decay and treatment response. We work in the areas of Medical Image Segmentation and Image Registration.

**Debapriya Basu Roy**
Email: dbroy24@gmail.com
Joined the department in December, 2014

***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.*

***Supervisor: Dr. 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 netbanking 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 involve 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 have 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 cannot 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 etc. 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 etc. 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 provide 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**
Joined the department in January 2014

***Debashis Mukherjee*** *received the BE and MSc (Engg.) degrees in mechanical engineering from Javadpur University, in 1996, and IISc, Bangalore, in 1998, respectively. He received his MTech degree in computer technology from computer science and engineering department in Jadavpur University, in 2013. Debashis was employed as software engineer/consultant with Macmet Interactive Tech., Kolkata, Lucent Tech., Bangalore, Sun Microsystems, Bangalore, Intel Tech., Bangalore, Evolving Systems Networks, Bangalore, IBM, Kolkata, and Cognizant Tech. Systems, Kolkata since 1999 through the decade. From 2014, Debashis is a student in the computer science and engineering department at IIT, Kharagpur, pursuing his PhD under the supervision of Prof. Rajib Mall. Debashis is investigating into effective test coverage in program testing*

***Supervisor: Prof. Rajib Mall***

**Program Analysis and Testing**

Program analysis and testing using machine learning approaches.

**Devleena Ghosh**
Joined the department in June 2016

***Devleena Ghosh*** *received B.E. degree in Computer Science & Technology from Bengal Engineering and Science University, Shibpur in 2010. From July 2010 to June 2011, she was a Junior Research Fellow in the Department of Computer Science and Engineering in IIT Kharagpur. She completed her M.Tech in Computer Science and Engineering from IIT Kharagpur in 2013. From August 2013 to December 2015, she worked as a Software Development Engineer at Microsoft India, Hyderabad. Since January 2016 she has been a Ph.D. student in the Department of Computer Science and Engineering. She has worked in logic simulation, e-learning and application of formal verification in railway interlocking systems. Currently her research interest lies in computational modelling of physical systems.*

***Supervisor: Chittaranjan Mandal***

**Dhiman Saha**
Email: crypto@dhimans.in, saha.dhiman@gmail.com
Joined the department in: July 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.*

***Supervisor: Prof. Dipanwita Roychaudhury***

## 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. Available at http://competitions.cr.yp.to/caesar.html



**Durga Prasad Sahoo**
Email: dpsahoo.cs@gmail.com
Joined the department in January 2012


***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 and Engineering 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 physically unclonable functions, cryptographic engineering and secure embedded system design.*

***Supervisors: Prof. Rajat Subhra Chakraborty, Prof. Debdeep Mukhopadhyay***

**Design and Analysis of Composite 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. As a part of my research, I am attempting to construct modeling-attack resilient PUF by the composition of standalone existing PUF designs and a mathematical framework to evaluate the robustness of PUF design against modeling attack.

**Gaurang Panchal**
Email: gp.citc@gmail.com
Joined the department in July 2012

***Gaurang Panchal*** *received the B.E. degree in Information Technology from the Saurashtra University, in 2003, and the M.E. degree in Computer Engineering from Dharmsinh Desai University, in 2007. He is an Assistant Professor in Charotar University of Science and Technology, Gujarat. Presently, he is working toward the Ph.D. degree (under Quality Improvement Program) at the Department of Computer Science and Engineering, IIT, Kharagpur. His research interests include Biometric Security and Cryptography.*

***Supervisor: Prof. Debasis Samanta***

**Fingerprint Biometric-Based Approaches to Remote User Authentication Schemes**

The use of information exchange across the Internet, and storage sensitive data on open networks, cryptography is becoming an increasingly important future of data security. Feature extraction and detection are an important component of fingerprint verification. Some existing system use fingerprints database, fingerprints feature database with different instance for authentication but our Proposed approach doesn't use any database for authentication. Same user can encrypt and decrypt his message/data using his fingerprints without using any database for authentication. The main focus of proposed approach is on similar feature extraction and Cryptography key generation using Biometric fingerprint. One user will generate unique cryptographic key using his fingerprint. Next time user will generate another cryptographic key and he can decrypts message using same fingerprints.

Messages encrypted with keys based on randomness have the advantage that there is theoretically no way to "break the code" by analyzing a succession of messages. Each encryption is unique and bears no relation to the next encryption. The decrypting party must have access to the same key used to encrypt the message and this raises the problem of how to get the key to the decrypting party safely or how to keep both keys secure. So, the idea is to use the same cryptographic key for same session and another key for different session. So same user can encrypt and decrypt message using his fingerprints in same session only. Here, we present a proficient approach for the secure cryptographic key generation based fingerprint image. Our Proposed System focus on "One User, Different Session, Different Keys" to encrypt and decrypt message.

**Ilora Maity**
Email: ilora_maity@yahoo.com
Joined the department in: July 2015

***Ilora Maity****, is presently pursuing he Doctor of Philosophy (PhD) degree from the School of Information Technology, Indian Institute of Technology Kharagpur, India. Her current research interests include Wireless Sensor Networks and Big Data Networking. She has completed her M. E. degree in Computer Science and Engineering from Bengal Engineering and Science University, Shibpur, India in 2011. Her M. E. Thesis is entitled as "A Cellular Automata based Scheme for Diagnosis of Faulty Nodes in WSN". She received her Bachelor of Technology degree in Computer Science and Engineering from MCKV Institute of Engineering, West Bengal University of Technology, India in 2008. She has worked as Technical Analyst of Banking & Financial Services in Cognizant Technology Solutions India Pvt. Ltd. Kolkata, India from September 2011 to July, 2015. She is a member of Smart Wireless*

*Applications & Networking (SWAN) Research Group, Indian Institute of Technology Kharagpur.*

***Supervisor: Prof. Sudip Misra, Prof. Chittaranjan Mandal***

**Addressing Scalability Challenge of SDN**

Increasing scalability of SDN for big data processing.

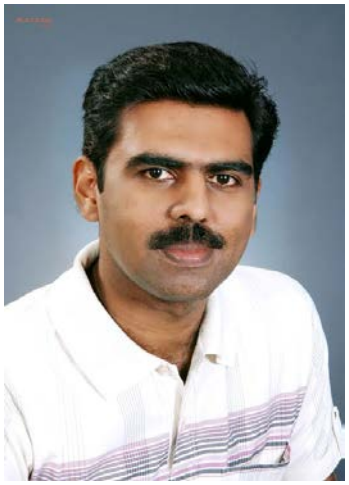
**Jasabanta Patro**
Email: jasabantapatro@gmail.com
Joined the department in: December 2015

***Jasabanta Patro*** *has completed his B.Tech in Computer Science and Engineering from BPUT, Rourkela in 2013 and M.Tech in Bioinformatics from department of Mathematics and Computer Application of MANIT Bhopal in 2015. There after he joined at IIT Kgp as a PhD scholar in Department of Computer science and Engineering in Dec 2015 to pursue my research.*

***Supervisor: Dr. Animesh Mukherjee***

**Analyzing Social Dynamics of Code Mixing and Code-Borrowing**

The dynamics of a language plays an important role in effective user query processing, information retrieval, and natural language processing. Some of the factors that can influence this dynamicity stem from the social interactions among speakers with different native languages and the extent to which words/phrases are adopted by them from other languages. Detailed investigation of such dynamics is only recently becoming possible due to the availability of data from different social media platforms that reflect various levels of code-switching, code-mixing, and code borrowing before a linguistic change is formally admitted into a lexicon. The primary goal of this research would be to investigate the dynamics of code-mixing, code-switching and code-borrowing and how each of these are socially influenced. Such studies can have a very strong impact on how to handle IR and NLP applications in an extensively multilingual setting.



**John C John**
Email: johncyriljohn@gmail.com
Joined the department in: July 2014

***John C. John*** *received the MTech degree from IIT, Kharagpur, in 2012, and is currently working toward the PhD degree. His research interests include access control, distributed systems, and data mining.*

***Supervisor: Prof. Shamik Sural, Prof. Arobinda Gupta***

**Expressing Access Control Security in Multiple Distributed Environments**

Development and maintenance of secure information systems is a challenging goal in today's distributed computing environment. Rapid expansion of distributed environments such as cloud, Internet of Things (IoT) and smart environments makes the systems increasingly heterogeneous and applications overly complex. The purpose of collaboration in multiple distributed environments is to share information and to exchange resources across organizational boundaries. The types of collaborations can generally be classified as Federated, Loosely Coupled and

Ad hoc collaborations. The security goals of such multi-domain environments are to protect resources from unauthorized accesses and to ensure availability of services to the authorized users. The security services required to meet these security goals are authentication and access control. Security requirements of such systems can be specified as security policies. The autonomous and heterogeneous natures of policies of different domains often lead to conflicts among policies. The policy conflicts which violate the principles of security under collaborations among multiple domains are called security conflicts. Complete disclosure of access control policies of participating domains is essential for federated type of collaborations. In this type of collaboration, a mediator domain is used to compose a global access control policy and the applications should be developed according to the global policy. Loosely Coupled collaborations are work flow based applications. In this type of collaboration, a global directory service can be used to store resources, interfaces and access control policies. Tasks in a work flow must be verified with the policies of the resources. Applications that run on on-demand basis require lowest degree of interoperability and which uses ad hoc collaborations. Such applications run on mediator free environments. They use either use trust based approaches or access history based approaches to ensure secure collaborations.

**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 and Facebook 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, the Twitter OSN 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 the 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 and 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, not all information obtained through OSNs are trustworthy. Again, it is a challenge to extract important updates about an ongoing event (known as situational updates) from among the large amounts of generic comments being posted. Hence, 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 situations in countries such as 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.

**Madhumita Mallick**
Email: madhumitamallick@iitkgp.ac.in
Joined the department in: August 2015

***Madhumita Mallick*** *graduated (B.E) from Jadavpur University in Computer Science and Engineering in 2013 and finished M.Tech in 2015 from IIT Kharagpur. She has started my PhD under professor Niloy Ganguly.*

***Supervisor: Prof. Niloy Ganguly***

**Demultiplexing Activities and storage reduction in IoT enabled smart home**

My work involves attempt to demultiplex sensor generated events streams to identify complex activities and understand the behavior of sensor streams to improve daily living such as employing voice assistance or prompting service accurately. We also leverage and integrate IoT research with Data mining and analysis, storage systems where we can handle the huge amount of data generated by IoT sensors and intelligently store and analyse them by determining the correlation among sensors.

**Mahendra Pratap Singh**
Email: mp_singh@sit.iitkgp.ernet.in
Joined the department in: July 2013

***Mahendra Pratap Singh*** *received his B.Tech. in Computer Science and Engineering from Uttar Pradesh Technical University, Lucknow in 2005 and M.Tech. in Computer Science and Engineering from Karunya University, Coimbatore in 2007. He joined NIT Karnataka as Assistant Professor in the department of Computer Science and Engineering in January 2009 and continues to be part of the institute. Since July 2013, he is a research scholar in the school of Information Technology in IIT Kharagpur. His research interests are in the areas of Computer and Information Security.*

***Supervisor: Prof. Shamik Sural***

**Managing Multi-dimensional Multi-granular Security Policies using Data Warehousing**

Over the past few decades, sophisticated access control models have been proposed to take into account different dimensions such as time, space, role, context, attribute, etc. These enable specification of fine grained access control policies and can better express evolving organizational needs. However, the key problem is that, there is no comprehensive solution that can uniformly specify, evaluate, maintain and analyze these multitudes of policies in a consistent fashion. In this work, we show that specifying and enforcing access control policies of multiple granularities and dimensions can be transformed to the problem of specifying data of multiple granularities and dimensions. We show how the techniques and tools developed to specify, query and maintain data warehouses can be employed to solve complex access control problems. Specifically, we develop a unified schema to represent various access control policies such as Discretionary Access Control (DAC), Mandatory Access Control (MAC) and Role Based Access Control (RBAC) policies, and show how they can be automatically evaluated.

**Nabiul Islam**
Email: nabiuli@sit.iitkgp.ernet.in
Joined the department in December 2010

***Nabiul Islam*** *received the B.Tech. and M.Tech. degrees in computer science and engineering from the University of Calcutta, India. He is currently working toward the Ph.D. degree at IIT Kharagpur, Kharagpur, India. His research interests include design and analysis of energy-efficient protocols in the area of energy constrained networks such as nano-networks, wireless body area networks.*

***Supervisor: Prof. Sudip Misra***

**Characterizing Collision and Optimizing Energy consumption in Nanoscale Communication Networks**

Nanoscale communication networks (henceforth termed as "nanonetworks") consist of at least one synthetic network component of size ranging 1–100 nm and exploit nanoscale properties of those nano-components, and incorporate the basic elements of information theory—transmitter, message, message carrier, medium, and receiver. Limited energy capacity and small magnitude of harvested energy of such nanonetworks render the design of robust networking protocols challenging. Furthermore, potential applications based on nanonetworks are expected to adopt multi-hop communication strategy due to the limited communication range and stringent power budget of such nanonetworks. Therefore, the study on characterization of the phenomenon of collision, and optimization of energy consumption of such nanonetworks is of paramount importance for providing foundations on enabling robust multi-hop nanoscale communication networking.

**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***

**Indian Monsoon Modelling**

Climate Informatics is the branch of study lies at the intersection of climate science, computer science and information science. Climate Science relates to defining weather condition averaged over a period of time. Computer Science deals with extracting useful pattern in the climate or predicting the climate change. Information science brings broader societal and philosophical questions of the nature of information and why people need it.

Climate analysis task can be modeled from two directions - machine learning based model and physics based model. Machine learning approach is directed at moving from data towards knowledge; it outputs a mathematical model that describes the discovered relationships and pattern in the data. However, physics based model moves from knowledge (in form of physical theories of climate process) towards data. It is a way of exploring how well current theory explains the data. Clearly, two approaches are complementary; it is required to combine them together to build a strong bridge between data and wisdom.

The problem of identification of climate indices and study and modeling of Indian monsoon system is focused. Agriculture is the backbone for stability in India. It relies heavily on the monsoon season since the irrigation system is not proper throughout the country. Proper planning and provision are required for devising agricultural strategies. Small variation in the timing and quality of Indian monsoon has immense potential to impact agricultural output. Thus, prior knowledge of monsoon behavior for a year will help agricultural policy makers to devise proper scheme for best growth of appropriate crops. Different statistical and machine learning approaches are applied to identify different Climate Indices affecting Indian monsoon. The techniques are also utilized to study Indian monsoon pattern and finally to devise a prediction system for Indian monsoon.

**Narendra N P**
Email: narendrasince1987@gmail.com
Joined the department in December 2011

***Narendra N P*** *received B.E degree in electronics and communications engineering from Siddaganga Instituite of Technology (SIT), Visvesvaraya Technological University, India, in 2009 and M.S degree in information technology from Indian Institute of Technology Kharagpur, India in 2011. He is currently pursuing Ph.D. degree at the Indian Institute of Technology Kharagpur, India. His research interests include speech signal processing, speech synthesis and pattern recognition.*

***Supervisor: Prof. K. Sreenvasa Rao***

## Source Modeling for Improvement of Quality of HMM-based Speech Synthesis

Speech is the most natural way for humans to communicate with each other. Synthesis of artificial human speech provides efficient human-computer communication. Nowadays, the speech synthesis systems are widely used in various applications such as screen readers for visually challenged people, speech interface for mobile devices, navigation, and personal guidance gadgets. As humans are very sensitive in perceiving even the slightest distortions in the speech signal, the speech synthesizers with suboptimal quality make them unfit for usage in commercial applications. The main goal of this work is to improve the quality of HMM-based speech synthesizer by efficiently modeling the source or excitation signal.

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

***Supervisor: Prof. Partha Bhowmick***

***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.*

**Parantapa Bhattacharya**
Email: parantapa@cse.iitkgp.ernet.in
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, Prof. S. K. Ghosh***

## 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



**Pradeep R**
Email: pradeep_raj31@iitkgp.ac.in
Joined the department in December 2014


***Pradeep*** *is doing his research in the area of Automatic Speech Recognition (ASR) . His areas of interests are Speech signal processing, Probabilistic Graphical Models and Information retrieval. He did my Mtech in Siddaganga Institute of Technology, Tumkur, Karnataka in the field of Signal processing. His undergraduate was from Visvesvaraya Technological University (VTU) in the field of Electronics and Communication engineering.*

***Supervisor: K Sreenivasa Rao***

**Speech based access of Agricultural commodity price information retrieval**

Automatic Speech Recognition (ASR) aims at extracting useful information from a stream of speech and figures out what a person is saying. Considerable progress has been made in ASR research over the past few decades. However only a few work has been reported in the area of ASR in Indian Languages where there is a huge dialect variations among different regions of the states. Also ASR technique is being less deployed to adopt in the practical environments because of the lack of robustness in performance of the system. India being developing nation, work has to be concentrated on those backbones of the nation, the farmers. The farmers in India are expected to be benefited from both increased production and higher price realizations — leading to rising rural incomes and declining poverty rates. But they are not getting enough information about the current price that Government provides for the commodities because of the lack of information for each commodity in different markets of a particular state. Even though there is a AGMARK website which provides the price information based on the daily update, the farmers are still not familiarize with the use of Internet access and not affordable to smart phones. So an easy way must be to ask for commodity information, recognize speech and respond the price information. In this work, the focus is on Speech based access of Agricultural Commodity price information for the state of Bihar.

**Pritam Bhattacharya**
Email: lord.pritomose@gmail.com
Joined the department in December 2014


***Pritam Bhattacharya*** *received his B.Tech. (Computer Science and Engineering) degree in 2010 from Institute of Engineering and Management (IEM) under West Bengal University of Technology (WBUT). Subsequently, he joined the School of Technology and Computer Science at the Tata Institute of Fundamental Research (TIFR) in Mumbai, and obtained his M.S. from there in January 2014. He is currently pursuing PhD at the Department of Computer Science and Engineering in IIT Kharagpur*.

***Supervisors: Sudebkumar Prasant Pal, Subir Kumar Ghosh***

**Approximation Algorithms and Inapproximability Results for Art Gallery Problems**

I am broadly interested in the design and analysis of approximation algorithms for variants of the art gallery problem, which is a classic problem in the domain of computational geometry. It originates from the real-world problem of finding the minimum number of guards (or cameras) required to have an art gallery (represented by a polygon) under complete surveillance. Discovering good algorithms for solving these problems leads to several practical applications, particularly in the areas of military surveillance and robot-motion planning. Unfortunately however, most standard variations of the art gallery problem have been established to be NP-hard, implying that exact solutions for them cannot be computed efficiently. Therefore, we focus on the next best thing - designing efficient algorithms that output an approximate solution, but at the same time provide a relative performance guarantee that the value of the solution is within some (preferably constant) factor of the optimal value. While trying to improve the best known approximation ratio till date, we make parallel efforts to try and establish inapproximability bounds on these problems.

Recently, we designed a quadratic time 6-approximation algorithm for finding the minimum number of vertex guards required to guard a polygon without holes that is weakly visible from an edge, and proving an inapproximability result for the same problem in the case of polygons containing holes. The importance of our result lies in the fact that it proves, for a special class of polygons, a long-

standing conjecture by Ghosh regarding the existence of constant factor approximation algorithms for vertex guarding. Currently, we are focused on extending our earlier results to obtain constant factor approximation algorithms for finding the minimum number of vertex guards required for more general classes of polygons, such as monotone polygons and LR-visibility polygons. The pinnacle of success along this path would be to obtain a constant factor algorithm for all simple polygons without holes, thereby settling the decades-old conjecture by Ghosh completely. In parallel, we are also investigating the problem of vertex guarding in a setting where the guards are allowed to see points within the polygon directly as well as via a single diffuse reflection along one of the edges, which act as mirrors.

**Priyanka Sinha**
Email: priyanka.sinha.iitg@gmail.com
Joined the department in July 2012

***Priyanka Sinha*** *is a PhD student in Computer Science and Engineering at IIT Kharagpur and a scientist at Innovation Lab, Tata Consultancy Services Limited, Kolkata. Her focus area is Text Mining. She obtained a Bachelor of Technology degree from Indian Institute of Technology Guwahati, in Computer Science and Engineering and Master of Science degree from Auburn University, in Electrical and Computer Engineering.*

***Supervisors: Prof. Pabitra Mitra, Dr. Lipika Dey***

**Identifying Personality Traits from Enterprise Social Network for Mining Enterprise Group Behavior**

It is well known that modern organizations rely heavily on unstructured information to capture expertise and knowledge that otherwise exist in the minds of its employees. Computational linguistics and text mining techniques have made it possible to analyze and extract meaningful insights from the unstructured text collections and transform them into actionable intelligence as and when required. In this work our aim is to look at methods and techniques that can be employed to exploit content from enterprise social media with the explicit purpose of understanding individual behavioral traits and group interactions. It is expected that such analysis can be further used to simulate enterprise workers and study group dynamics for better team selection and management. Understanding group dynamics can contribute towards better group formations in future to accomplish tasks more efficiently, amicably and effectively. It can also help in automated monitoring of text communications to make it more effective.

**Rajendra Prasath R**
Email: drrprasath@gmail.com
Joined the department in: January 2009

***Rajendra Prasath R*** *received M.Sc (Mathematic)] from Ramanujan Institute for Advanced Study in Mathematics, M.Tech (CSE) from Indian Institute of Technology, Kharagpur and Ph.D (Mathematics-Computer Science) from University of Madras. Rajendra started his research career with a guest faculty position at University of Madras in 1998. During 2004-2006, he worked as an Assistant Professor at MNMJEC under Anna University, Chennai. Later Rajendra joined Communication Empowerment Laboratory of IIT Kharagpur as a Senior Project Officer. During August 2009 – September 2010, Rajendra was associated with 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 IIT KGP) as a part of DIT, Govt. of India sponsored research work. Presently Rajendra is a Technical Editor of the journals: Advances in Information Sciences and Journal of Computer Science. 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 member of World Federation on Soft Computing, Information Retrieval Facility – Vienna, International Rough Set Society (IRSS) – Warsaw and Information Retrieval Society of India. His research interests include cross lingual information retrieval, textual case based reasoning, machine learning and distributed algorithms for message passing systems.*

***Supervisor: Prof. Sudeshna Sarkar***

**Rajib Lochan Jana**
Email: rajib.jana@cse.iitkgp.ernet.in
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 before join the department. 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, Prof Pallab Dasgupta***

**Guided Reconstruction of Corner Cases in Architectural Validation of processor design**

Functional verification is widely acknowledged as one of the main challenges in the design cycle of modern microprocessor based systems. The industrial practice for functional verification of microprocessors relies heavily on extensive simulation. In a simulation based verification environment, the RTL is simulated with test programs with the hope that any design fault shall be revealed either by failure of correctness assertions or by back propagating through a simulation trace that generates a functionally wrong output. When such design bugs are found, the designer patches the RTL descriptions and restarts the verification process in order to check whether the bug fix is complete and correct. However, the bug fix can be local in nature in the sense that the bug may possibly manifest itself in an alternate execution trace. The present work leverages AI planning to develop techniques for automatic construction of test programs for sensitizing deep architectural bugs by reproducing a bug scenario as different possible sequences of micro-architectural events given that the scenario was initially observed as one such sequence in a simulation trace. Automated generation of such test programs 1) help to evaluate the robustness of a given bug fix or alternatively 2) identify the root cause of the bug so that a proper fix can be carefully planned.

**Rajorshee Raha**
Email: rajorshee.raha@cse.iitkgp.ernet.in
Joined the department in June 2013

***Rajorshee Raha*** *received B.Tech(ECE) degree and M.tech(ECE) degree from West Bengal University of Technology(WBUT), Kolkata in 2009 and 2011 respectively. From July 2013, he has been a Research Scholar in the Department of Computer Science & Engineering. His primary research interests are Formal Verification and Embedded Real Time Control Systems.*

***Supervisors: Prof. Pallab Dasgupta, 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 is 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. ˚Astr¨om 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*** *received a B.Tech. degree in Information Technology from Kalyani Government Engineering College, under West Bengal University of Technology in 2009. From July 2009 till July 2010, she worked in Indian Statistical Institute, Kolkata, as a Project Linked Personnel. She received an M.E. degree in Computer Science and Engineering from Bengal Engineering and Science University, Shibpur in 2012. Since July 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 Digital Geometry, Image Processing, Computer Graphics, and Discrete Geometry.*

***Supervisors: Prof. Partha Bhowmick***

**On Discretization of Sphere and Related Problems in 3D Integer Space**

The literature of digital geometry as of now contains a rich collection of work related to discretization of different geometric primitives and general surfaces in the digital or integer space. However, characterization, modeling, and algorithmic issues in connection with discrete spheres and its immediate derivatives like spherical paths and circles were not yet studied up to their merit. Under the supervision of Dr. Partha Bhowmick, I worked on several theoretical problems related to discretization of sphere and 3D geometric primitives on discrete spherical surface. During the course of my PhD, we have addressed some of the above-mentioned issues and present several new theoretical findings, efficient algorithms, and computational aspects concerning the aforesaid primitive objects in the integer space. We have first shown how elementary number-theoretic analysis can lead to characterization of naive and standard models of discrete sphere, which, in turn, aids in designing efficient algorithms for their construction using simple integer operations. Based on this characterization, we have worked out certain effective techniques for construction of discrete spherical geodesic paths and circles that are taken from the intersection of a discrete sphere and a discrete geodesic plane.

As a natural follow-up of this problem, we have done a characterization of different topological classes arising out of the combination of discretization models of the concerned sphere and geodesic plane. We have also visited the problem of construction of non-geodesic circles and have established some theoretical results related to this. As a further improvement, we have introduced the idea of functional gradation of quadraginta octants (symmetrical parts) of discrete sphere. We have shown how it helps in designing a fairly simple algorithm for construction of a special kind of 3D circle that maintains a better symmetry as well as bounded distance from the underlying real sphere and real plane.

To address the connectivity issues of curves defined on a sphere in the discrete topological space, we have proposed a new model of discrete sphere called graceful sphere. We have investigated the

properties of a discrete spherical geodesic path between two voxels and have shown that discrete 3D circles, circular arcs, and Mobius triangles are all constructible on a graceful sphere, with guaranteed minimum thickness and desired connectivity in the topological space. To demonstrate the applicability of integer algorithms in rapid prototyping, we have also proposed an efficient layering algorithm for construction of thick-walled discrete sphere.

**Rohit Verma**
Email: rohitverma.kgp@gmail.com
Joined the department in January 2016

***Rohit Verma*** *passed my B.Tech in the field of Computer Science and Engineering, from National Institute of Technology, Durgapur in 2013. Currently, he is working in the the research area of Smartphone Computing for my PhD work.*

***Supervisor: Prof. Sandip Chakraborty, Prof. Bivas Mitra***

**Energy Efficient Navigation Systems**

Navigation, be it pedestrian or vehicular is of prime importance now-a-days. Vehicular navigation, although in a very good stage in developed countries, is marred by several problems. These bring out a whole bunch of interesting research problems which can help not only the common public in developing countries but also of the developed countries. The first set of problems fall into this category of outdoor navigation and development of improved systems and maps for the same. The next set of problems decided upon is related to pedestrian localization where we plan to give a complete interference free navigation experience to the user. The idea of actuated navigation comes into play here.

**Sandipan Sikdar**
Email: sandipansikdar@cse.iitkgp.ernet.in
Joined the department in: January, 2013

***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 time-varying networks and delay-tolerant networks.*

***Supervisors: Prof. Animesh Mukherjee, Prof. Niloy Ganguly***

**Evolution of structural properties in temporal networks**

Most of the initial works attempted to study temporal networks by aggregating the network across all times and then analyzing this aggregated network. This strategy however hides the time ordering of the nodes and edges which has a significant role in the understanding of the true nature of these temporal networks. Researchers have subsequently come up with techniques addressing this issue. In this work we propose a different approach to analyzing temporal networks by mapping it to a time series and thereby allowing us to apply the known analytical tools for time series prediction for predicting the dynamical properties of temporal networks which would otherwise have been extremely difficult using standard methods of network generation at least in the context of temporal networks. We propose a framework for converting a temporal network to a time series. A temporal

network can be considered to be a set of static snapshots collected at consecutive time intervals. We also identify nine properties of a static complex network and measure them for each snapshot across all the time points. Hence, we obtain a modified representation of a temporal network which is a set of points ordered in time or equivalently a time series. For the prediction purpose we use Auto-Regressive-Integrated-Moving-Average model (ARIMA). In ARIMA modeling the input is a time series and the output is an auto-regressive equation with the help of which we can predict the value at a future time step. For ARIMA model to work, the time series must be stationary. However, most of the networks in real-world are not perfectly stationary. Therefore, we divide the time series into short stretches that are stationary and then perform our predictions on these smaller stretches. In order to find the right size for one such stretch we use the auto-correlation plots of the time series which measures the correlation of the series with itself at different lags. Once the window (let its size be l) is set we proceed for the prediction. For predicting the value at any timestep we feed the ARIMA model with previous l values and then obtain the prediction. We applied our framework to two real-world datasets SIGCOMM 2009 and INFOCOM 2006 . Initial results indicate significant accuracy of prediction in both the cases. It can be noted that this is equivalent to having a generating model for the temporal network and thereby predicting the properties of the network. We now plan to analyze these time series in frequency domain as well through spectrogram analysis and use it to further improve the prediction accuracy. We further plan to leverage this initial framework to analyze the temporal structures of various other networks ranging from human-contact networks to scientific citation networks to different online social networks and finally come up with a much more generic model. In addition, we plan to apply this framework to tasks like link prediction and recommendation.

**Samaresh Bera**
Email: samareshbera91@gmail.com
Joined the department in: January, 2015

*Samaresh Bera is presently pursuing his Ph.D. from the Department of Computer Science and Engineering, Indian Institute of Technology Kharagpur, India. Besides, he is working as a Senior Research Fellow in a research project entitled "An Indigenous Framework for Authenticity, Integrity and Non-Repudiation in Data Communication", DRDO, Govt. of India. He received his MS (by research) degree from the School of Information Technology, Indian Institute of Technology, Kharagpur in 2015. He received the B.Tech degree in Electronics and Communication Engineering from West Bengal University of Technology, India in 2011. His current research interests include software-defined networking, smart grid communications and networking, Cloud computing. He has published several journal and conference papers. He serves as a TPC member of IEEE ScalCom-2014, ICACIE 2016, and IEEE TechSym-2016. He is a reviewer of IEEE Trans. on Smart Grid, IEEE Trans. on Cloud Computing, IEEE Trans. on Emerging Topics in Computing, IEEE Trans. on Cybernetics, IEEE Communications Magazine, and IEEE Systems Journal to name a few. He is a student member of IEEE.*

***Supervisor: Dr. Sudip Misra***

**Software-Defined Networking for Internet of Things**

The inherent features of internet of things (IoT) opens a new direction to fulfill the objectives toward fully connected world in near future. The IoT environment is comprising of wireless sensor networks (WSNs) and heterogeneous nodes in both the infrastructure-based or the infrastructure-less (i.e., ad-hoc manner) fashion with the capability of establishing smart systems (such as smart health-care, smart energy system, video surveillance, and intelligent transportation systems). Consequently, adequate networking aspects need to be enabled to support such devices in real-time in a ubiquitous and seamless manner. Therefore, the traditional network architecture needs to be modified to enable the networking aspects in the connected world in which the huge number of devices are expected to

participate.

Concurrently, software-defined networking (SDN) is one of the promising approaches to support user-defined networking aspects, while separating the control plane from the data plane. Thus, we have a global view of the network and can control the network traffic according to different applications. Additionally, it is also possible to use the same physical devices to support different applications, while modifying the control strategies. However, existing works on SDN mostly focused on high-speed network platforms such as data center networking and certain extends to wifi enterprise networks, and are applicable to wired networks.

In view of the above, he is focusing on the software defined networking aspects in the future internet of things architecture while addressing different challenges of implementing SDN in both the infrastructure-less and infrastructure-based scenarios.

**Sankaraganesh Jonna**
Email: sankar9.iitkgp@gmail.com
Joined the department in: December, 2012

*Sankaraganesh Jonna received a B.Tech. degree in Information Technology from Bapatla Engineering College, Andhra Pradesh in 2010. He received an M.Tech. degree in Computer Science and Engineering from Velagapudi Ramakrishna Siddhartha Engineering College, Jawaharlal Nehru Technological University Kakinada, in 2012. Since December 2012, 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, Image Processing, Machine Learning and Optimization.*

***Supervisors: Dr. Rajiv Ranjan Sahay***

**Image Super-resolution and De-fencing**

In real-world scenarios, images or videos taken at public places using inexpensive low-resolution cameras, such as smartphones are also often degraded by the presence of occlusions such as fences/barricades. Finer details in images captured using such low-end equipment are lost due to blurring and under-sampling. Compounding this problem is missing data due to the presence of an intervening occlusion between the scene and the camera such as a fence. To recover a fence-free high-resolution image, we use videos of the scene captured by panning a hand-held camera and model the effects of various degradations. We divide the problem of image super-resolution de-fencing into three sub-problems. Initially, we obtain the spatial locations of fences by proposing diverse set of algorithms using shape, depth and blur as cues. Subsequently, the shifts between the frames has been estimated using optical flow. Finally, the underlying high-resolution fence-free image is modelled as an inverse optimization framework and solved. In this work, we try to evaluate the proposed algorithms on the state-of-the-art and our datasets.

**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 various components 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.

**Satendra Kumar**
Email: satendra.cse@gmail.com
Joined the department in: July, 2015

*I am a first year Ph.D student in Department of Computer Science and Engineering at Indian Institute of Technology Kharagpur, India. Along with this, I am affiliated to Smart Wireless Applications & Networking (SWAN) Lab under the supervision of Prof. Sudip Misra. I have completed my M.Tech in Computer Technology from National Institute of Technology (NIT) Raipur, with Gold Medal. Prior to joining Ph.D, I have served as an Assistant Professor in the Department of Information Technology at Bengal College of Engineering and Technology (BCET), Durgapur.*

***Supervisors: Prof. Sudip Misra***

**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.*

***Supervisors: 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 criterion 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 proves 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.

**Shrutilipi Bhattacharjee**
Email: shrutilipi.2007@gmail.com
Joined the department in: July, 2011

*M.Tech. University: National Institute of Technology Durgapur*
*Branch: Information Technology; Year: 2011*

*B.Tech. University: West Bengal University of Technology*
*Branch: Information Technology; Year: 2009*

***Supervisors: Prof. Soumya K. Ghosh***

**Prediction of Meteorological Parameters and Knowledge Discovery in Geographic Information System**

Meteorological attributes, related to earth surface, are considered to be the important factors for modeling climate dynamics. Modeling land-atmospheric interaction for these attributes, nearby to the earth surface is mandatory to achieve better precision for their prediction, as well as for investigating spatio-temporal atmospheric patterns. Examples of these attributes include land surface temperature, vegetation index, built-up index, etc. According to NASA Earth Observatory, the land surface temperature is an influential factor for warmth rising of Earth's landscapes, and influential to determine the climate patterns. Our research work focuses on the prediction and forecasting of these meteorological attributes. We have proposed a new Kriging based spatial interpolation technique, namely Semantic Kriging, considering the semantic relationships among geospatial objects for better prediction.

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

*Shyantani Maiti received a B.Tech. degree in Computer Science and Engineering from MCKV Institute of Engineering in 2010 and M.E. degree in Computer Science and Engineering from Indian Institute of Engineering Science and Technology, Shibpur (Formerly Bengal Engineering and Science University, Shibpur) in 2013. She joined as a PhD scholar in the Department of Computer Science and Engineering in December 2013. Her research interest is in Bioinformatics.*

***Supervisors: Prof. Pralay Mitra***

**Protein machinery on Bacterial Chemotaxis**

Our research aims to study the proteins causing bacterial motility to favour chemotaxis in bacteria. The detailed mechanism about how a bacterium switches its flagellar rotational direction in response to attractants or repellants present in its surrounding environment is to be studied at the protein level. Monitoring and tracking of the trajectory of bacterial motility by biologists specifically for a given chemical gradient can be done easily if we get the deep insight into this mechanism of bacterial chemotaxis.

**Sikhar Patranabis**
Email: sikhar.patranabis@cse.iitkgp.ernet.in
Joined the department in: July, 2015

*Sikhar Patranabis completed his B. Tech in Computer Science and Engineering from the Indian Institute of Technology Kharagpur. He is the recipient of the President of India Gold Medal Award for the batch of 2015. He is currently pursuing his PhD at IIT Kharagpur. His research interests include cryptography and hardware security.*

***Supervisors: Prof. Debdeep Mukhopadhyay***

## Design of Public-Key Cryptosystems for Data Sharing on the Cloud

The recent advent of cloud computing has pushed the limits of data sharing capabilities for numerous applications that transcend geographical boundaries and involve millions of users. Governments and corporations today treat data sharing as a vital tool for enhanced productivity. Cloud computing has revolutionized education, healthcare and social networking. However, such applications are also vulnerable to attacks from malicious service providers and third party intruders that could lead to catastrophic consequences. In this dissertation, we aim to propose online data sharing schemes based on key aggregate cryptosystems with strong cryptographic properties that ensure data security without compromising on the scalability and efficiency of the system. We prove the indistinguishability based security and collusion resistance of our proposed schemes in the standard game-based cryptographic model. We further aim to use this scheme to design identity based online data sharing schemes that are practically deployable in real world data sharing scenarios.

**Soumadip Biswas**
Email: soumadip.b@iitkgp.ac.in
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 IIT Kharagpur. His research interests are in the areas of Computer Networks, Wireless networks and Software Defined Networking.*

***Supervisors: Prof. Arobinda Gupta, Prof. Sandip Chakraborty***

## Handover in High-speed Heterogeneous Wireless Networks

With many wireless radio technologies such as LTE, WiFi, Wimax and possibilities of upcoming radio access technologies(RATs), it is required to ensure that they can co-exist and work together. The network of all the technologies aka the heterogeneous wireless network, with their omnipresence, has potential to pose new challenges when it comes to provide seamless experience to the end user. Such a problem is the handover problem. While a mobile node moves from one point to another, it is very essential to make proper decisions to choose the next access point such that it gives the desired experience in terms of quality of service, energy efficiency etc. Also the decisions are to be made in such a way, so that the overall system throughput also maximize. With higher speed of the mobile node the problem becomes more challenging. It becomes more complex with addition of multiple RATs. This problem takes such a system of highly mobile users such as vehicles in a road network or in a train. The system also has multiple RAT components available. These nodes, being on a defined track has the opportunity of mobility prediction.

**Soumajit Pramanik**
Email: soumajit.pramanik@cse.iitkgp.ernet.in
Joined the department in: July, 2013

***Soumajit Pramanik*** *passed B.Tech from ST. Thomas' College of Engg. & Tech. in 2011 and M.Tech from Indian Statistical Institute, Kolkata in 2013. He is currently a Ph.D. student in the Department of Computer Science and Engineering, IIT Kharagpur, since July 2013.*

***Supervisors: Prof. Bivas Mitra.***

**Information Propagation in Multi-Layer Social Networks**

Information propagation is a very well-studied phenomenon. From long ago, people are trying to understand how a piece of information travels from one person to another. Two types of information flows which have drawn most of the attentions of the researchers, are i) knowledge information flow (flow of ideas, innovations etc. mainly among scientists) and ii) social information flow (flow of news, gossips, opinions etc.). In every information propagation, there exist some hidden factors which are generally dormant and not given much importance, but if handled carefully, they can play crucial roles in deciding the properties (like size, speed etc.) of the diffusion. In our 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. Banking on that knowledge, we want to build novel techniques to accelerate and expand an on-going information diffusion and deploy them in large scale for the benefit of end-users.

**Soumya Sarkar**
Email: portkey1996@gmail.com
Joined the department in: July, 2015

*B.Tech 2012 -- RCC Institute of Information Technology*
*M.Tech 2015-- IIT Patna*
*JRF --- July 2015, Present*

***Supervisors: Prof. Animesh Mukherjee***

**Analysis of Noise In Networks and Applications**

Developing algorithms which can find meaningful information from Complex Networks which have been disrupted by various external agents. Analyse stability of the results of network mining algorithms under circumstance of random change or targeted change.

**Soumyadeep Dey**
Email: soumyadeepdey@gmail.com
Joined the department in: July, 2012

*Soumyadeep Dey received his B.Tech. in Computer Science and Engineering from West Bengal University of Technology, Kolkata, and his M.E. from Indian Institute of Engineering Science and Technology, Shibpur in 2009 and 2011, respectively. Currently, he is a PhD student in Indian Institute of Technology Kharagpur. His primary research interests include image processing, pattern recognition and computer vision.*

***Supervisors: Prof. Jayanta Mukherjee, Prof. Shamik Sural***

**Preprocessing of Document Images**

Optical Character Recognition (OCR) systems are in demand for their application in automated document processing. Various stages of document image processing are data acquisition, preprocessing, feature extraction, classification and post processing. Among these stages, preprocessing is the preliminary step which transforms the data into a format convenient for the next stages of processing. Preprocessing is necessary to modify the data either to overcome deficiencies in

the data acquisition process due to limitation of the capturing device sensor, or to prepare the data for subsequent activities in the later stages of description, as the performance of the subsequent phases depends on the quality of input data.

**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 behavior 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 a well-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 behavioral specification (of the systems to be designed) with a view to optimizing time and physical resources. Behavioral verification involves demonstrating the equivalence between the input behavior 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 behavioral description, and exactly those, are captured by the output description. The input behavior 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 behavioral specification to the original one, also referred to in the literature as transformation validation and (2) comparison of timing performances of the behaviors 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 behaviors 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.



**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 Phylogenetics. His research focuses on algorithms for constructing phylogenetic supertrees, deriving species trees from a set of (incongruent) gene trees. He is a TCS research scholar.*

***Supervisors: Prof. Jayanta Mukhopadhyay***

### Species Tree from Incongruent gene trees due to Incomplete Lineage Sorting

Phylogenetic trees represent evolutionary relationships between 'taxa' (entities such as genes, populations, species, etc.). Every leaf of the tree uniquely represents one taxon. From a species set, their representative common gene (in the form of either nucleotide or protein sequences) is used to construct phyloegentic trees, often termed as the gene tree. Different genes from same set of species may generate different gene tree topologies, since different genes often exhibit different evolutionary histories among a group of species. Further, few genes may not cover all of the input species, resulting partial gene trees. One major reason of such conflicts among gene trees is the Incomplete Lineage Sorting (ILS) or deep coalescence (DC). Such discordance can be so high that no single gene tree topology predominates in the input gene tree set. Topology of the species tree, thus, often

considerably differs from the input gene trees. Our research focuses on analyzing such ILS based discordance among gene and species trees, and developing computationally efficient algorithms to derive species trees from a set of incongruent gene trees.

**Sreeja.S.R**
Email: getsreeja@gmail.com
Joined the department in: July, 2014

*I received my B.Tech in Information Technology and M.E in Computer Science Engineering from Anna University, Chennai, in the year 2010 and 2014 respectively. Now pursuing my Ph.D degree in the department of Computer Science and Engineering.*

***Supervisors: Prof. Debasis Samanta (Supervisor), Prof. Pabitra Mitra (Joint Supervisor)***

**Brain computer Interface augmented Human Computer Interface for people with Special Needs**

A significant part of our world today suffers from various disabilities. At 15% the number is humongously large to ignore. These people find it extremely hard to lead a normal life. While communication comes easy to the able-bodied, it poses a serious challenge to the disabled. For those people with severe physical disabilities, such as damage of limbs, brainstem stroke, spinal cord injury, cerebral palsy, amyotrophic lateral sclerosis (ALS) or other neuromuscular diseases, BCI is the only method to communicate. Currently, several functional imaging modalities like EEG, MEG, fMRI, etc., are available for research.

Electroencephalography (EEG) is unique and most often used, since it promises to provide high temporal resolution of the measured brain signals, relatively convenient, affordable, safe and easy to use BCI for both healthy users and the disabled. Recent advances in computer hardware and signal processing have made possible the use of EEG signals or “brain waves” for communication between humans and computers. Locked-in patients have now a way to communicate with the outside world, but even with the last modern techniques, such systems still suffer communication rates on the order of 2-3 tasks/minute. In addition, existing systems are not likely to be designed with flexibility in mind, leading to slow systems that are difficult to improve.

The purpose of my study is to develop an effective BCI-HCI application, for motor disabled people who can handle cognitive load, which makes most accurate and fast choice with minimum human interaction. Developing such application systems with better communication rates using brain signals provides these people a great opportunity to act independently.

**Subarna Chatterjee**
Email: chatterjeesubarna@yahoo.com
Joined the department in: July, 2013

*I, Subarna Chatterjee, am pursuing my Ph.D. under the supervision of Dr. Sudip Misra. My areas of research are cloud computing, wireless sensor networks, and Internet of Things.*

***Supervisors: Prof. Sudip Misra***

**Sensors-as-a-Service: Towards the Conceptualization of Sensor-Cloud**

The emergence of Wireless Sensor Networks (WSNs) has enhanced the standard of living of mankind

with the touch of advanced technology. However, all of the WSN-based applications are single-user centric, in which a user-organization owns and deploys its personalized sensor network and typically does not share the accessed data to another party (user/organization). Thus, generally, only user organizations that own a sensor network have satisfactory access to sensor data. Recent research works has conceived sensor-cloud architecture as a potential solution for traditional WSNs. The works have primarily focused on the principles, the dogma, and the challenges involved in this shift of paradigm. However, despite the upsurge in research on sensor-cloud, there lacks mathematically based theoretical works that can help in supporting performance evaluation and analysis of sensor-cloud based systems.

The proposed research focuses on the development of sensor-cloud infrastructure. The proposed research has been initiated in 2013 when all of the existing research works focused primarily on the dogma, the principles, and the conceptualization of sensor-cloud. However, research work that provide scientific and technological concreteness to the concept of sensor-cloud infrastructure were scarce. From an implementation point of view, we have identified the scope of technical and theoretical research in this domain to mathematically suggest the shift of paradigm from traditional WSNs. The goal of this research is to resolve the technical challenges and eventually build a fully-functional prototype of sensor-cloud. The proposed research has succeeded in building a partially-functional prototype of sensor-cloud infrastructure which currently the only available infrastructure rendering Se-aaS, to the best of our knowledge.

**Subhadeep Sarkar**
Email: subhadeepsarkarybs@yahoo.com
Joined the department in: July, 2013

*I, Subhadeep Sarkar, am pursuing Ph.D. under the joint supervision of Dr. Sudip Misra and Dr. Chandan Chakraborty. I have joined the Institution on July 2013. My Doctoral research area includes wireless body area sensors and cloud computing.*

***Supervisors: Prof. Sudip Misra, Prof. Chandan Chakraborty***

**Analysis of delay in IEEE 802.15.6 CSMA/CA standard**

I am working on analysis of delay and mitigation of starvation and indefinite delay in IEEE 802.15.6 CSMA/CA standard.

**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.*

***Supervisors: Prof. Arobinda Gupta***

## Distributed Algorithms on Dynamic Graphs

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 Dutta**
Email: sudakshina@cse.iitkgp.ernet.in
Joined the department in: 18th July, 2011

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

***Supervisors: Prof. Dipankar Sarkar***

## Validation of parallelizing transformations of sequential programs on arrays

The parallelizing compilers have 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 parallelization 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 such parallelizing transformations. We also localize faulty application of enabling transformations when more than one of them are applied.

**Sudipa Mandal**
Email: contacttosudipamandal@gmail.com
Joined the department in: July 2015

***Sudipa Mandal*** *completed her B.E from Jadavpur University in 2013. She completed her M.Tech from IIT Kharagpur in 2015. She is currently pursuing PhD from IIT Kharagpur.*

***Supervisors: Professor Pallab Dasgupta***

**Formal Methods for Verification of Power Management in Mixed Signal Design**

The increasing complexity and safety-criticality of modern systems has created a need for validation and safety assurance of designs based on formal analysis. Formal methods have been used to check functional correctness of systems using methods such as model checking and design intent verification. Apart from checking for functional correctness, performance parameters such as power, reliability etc. have also been verified in recent research works. Architectural Power Intent Validation is a significant area of formal verification research, in which a large repertoire of work already exists. This work studies power intent validation for purely digital power domains using UPF (Unified Power Format) specifications for expressing power intent. With the increase in integration, today most SoCs in use contain not only digital domains, but analog power domains as well, introducing a new dimension to the verification problem. This shifts the domain of formal verification from purely digital to that of mixed-signal verification of power intent, which is an entirely new line of research. The same methodologies employed for the verification of power intent of digital cannot be employed for the verification of mixed-signal, because the UPF standard does not provide structures for the specification of intent for mixed-signal, and no known techniques exist that can generate formal proofs of correctness of mixed-signal power intent specifications. Our work is focused on the architectural power intent validation of Analog Mixed Signal power domains, which is substantiated by our past experience working on the power intent validation of digital power domains and in the formal analysis of features for analog and mixed-signal systems. This report provides a high level outline of the strategy we intent on using toward this unique verification problem, along with an introduction to our past work on formal analysis of AMS features.

**Sukla Satapathy**
Email: sukla.iit@gmail.com
Joined the department in: July 2014

**Sukla Satapathy** received his M.Tech (CS) from Utkal University.

***Supervisors: Dr. Rajiv Ranjan Sahay***

### 3D shape reconstruction using Shape from focus

My research interest is 3D shape reconstruction using Shape from focus (SFF) method. Shape-from-focus is a method which estimates the 3D structure of an object by measuring the degree of focus from a stack of space-variantly blurred frames obtained due to relative motion between camera and the specimen. This is an inverse, ill-posed problem. From optimization point of view it can be categorized as total variation regularized optimization problem and Split Bergman technique can be used for solving it.

**Suman Kalyan Maity**
Email: sumankalyan.maity@cse.iitkgp.ernet.in
Joined the department in: July 2013

***Suman Kalyan Maity*** *received his B. Tech. degree in Computer Science and Engineering from NIT Durgapur in 2011 and his MS degree in Computer Science and Engineering from IIT Kharagpur in 2013. He is a recipient of Microsoft Research India PhD Fellowship. His research interests broadly include Social computation: with key focus on popularity of entities in social QA (Quora, Stack Overflow etc.), hashtag popularity and evolution of linguistic entities like lexical compounding, lexical blending on social media.*

***Supervisors: 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 is 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. 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. #KellyRipa and #CelebrationMonth make #KellyRipaCelebrationMonth; #WikipediaBlackout is formed from #Wikipedia and #Blackout; #OregonBelieveMovieMeetup is formed from #Oregon, #BelieveMovie and #Meetup; #Educational, #Ipad, #Apps together make #EducationalIpadApps etc. There are marketing strategic needs, needs for fulfilling communicative intents (affective expression, political persuasion, humor etc.) as well as spontaneous needs for use of hashtag compounds. For example, the e-commerce company Amazon used #AmazonPrimeDay to promote the discounted sale of its product. The hashtag is a compound of #Amazon and #PrimeDay whereas the individual hashtag #PrimeDay was also popular. So, there is a

trade-off whether to use hashtag compounds or the uncompounded constituents. Similarly, assume another scenario where an event is taking place, say the premiere of a movie 'The Imitation Game'. Here one can use both the hashtags #TheImitationGame and #Premiere or can use a hashtag compound #TheImitationGamePremiere. In this context, one needs to identify which version one should use so that the hashtag being used gains a higher frequency of usage in the near future. #CSCW2016 is being used to tag the activities taking place related to the 2016 CSCW conference. This is also a compound hashtag made of #CSCW and #2016 where #CSCW refers to all CSCW conferences and #2016 refers to all the events/activities going to take place in 2016. The hashtag #CSCW2016 is used for a more focused purpose and refering to only the 2016 edition of the conference whereas #CSCW could also have served the purpose. Hashtag compounds also serve the communicative intents like political campaign hashtags (#PresidentTrump = #President + #Trump : hashtag that shows support for Donald Trump for the 2016 US Presidential election). Hashtag compounding also happen spontaneously. These hashtags are generally conversational or personal themed hashtags like #TheBestFeelingInARelationship (#TheBestFeeling + #InARelationship), #ThrowbackThursday (#Throwback + #Thursday), #ComeOnNowDontLie (#ComeOnNow + #DontLie). In this work, we identify for the first time that while some of these compounds gain a high frequency of usage over time (even higher than the individual constituents) many of them are soon lost into oblivion. We focus and investigate in detail the reasons behind the above observations and propose a prediction model that can identify with 77.07% accuracy if a pair of hashtags compounding in the near future (i.e., 2 months after compounding) shall become popular. At longer times T = 6, 10 months the accuracies are 77.52% and 79.13% respectively. 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. As an additional contribution, we ask human subjects to guess whether a hashtag compound will become popular from the structural information of the hashtags. Humans can predict compounds with an overall accuracy of only 48.7%. Notably, while humans can discriminate the relatively easier cases, the automatic framework is successful in classifying the relatively harder cases.

**Sumana Ghosh**
Email: sumanaghosh@cse.iitkgp.ernet.in
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.*

***Supervisors: Prof. Pallab Dasgupta, Prof. Soumyajit Dey***

**Formal Verification of Real Time Embedded Control**

Software control is widely used today in embedded hybrid dynamical systems, such as automotive and avionic control systems. The increasing complexity of such systems and our reliance on these systems demand rigorous guarantees on the safety and correct operation of such control. Providing formal guarantees about the safety and reliability of such systems require accurate modeling and validation of the interaction between the software, the control architecture and the hybrid dynamical system being controlled. Ms. Ghosh aims to study the underlying formalism for model based design and validation practices in embedded system development and develop new formal methods, tools and practices for verifying closed loop software based control of hybrid dynamical systems.

**Sumit Goswami**
Email: sumit_13@yahoo.com
Joined the department in: December 2011

***Supervisors: Dr. Sudip Misra***

**Behavioral and Security Analysis of Future Generation Networks**

Public key infrastructure based security for low power sensor networks like ZigBee, 6LoWPAN and specific use WSN.

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

*I am a Ph.D. student in the Department of Computer Science and Engineering, IIT Kharagpur, since Jan 2015. My supervisors are Prof. Bivas Mitra and Prof. Niloy Ganguly. My research interest lies in the area of Mobile Networks and Applications.*

***Supervisors: Prof. Bivas Mitra, Prof. Niloy Ganguly***

**Inferring Emotion from Smartphone Usage**

I am working in the area of Mobile Affective Computing. Currently, I am focusing 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.

**Tamoghna Ojha**
Email: tamoghna.ojha@gmail.com
Joined the department in: July, 2014

***Tamoghna Ojha*** *is currently pursuing PhD at the School of Information Technology, Indian Institute of Technology Kharagpur. He has completed MS from the Indian Institute of Technology Kharagpur in 2014. His research interests are in Internet of Things (IoT), sensor-cloud, mobile computing, underwater acoustic networks. Besides, he has several years of research experience working on research projects funded by different agencies such as ITRA and DeitY, Govt. of India. Previously, he has received the Post Graduate Diploma in Embedded Systems from CDAC, Mohali in 2009, and B. Tech in Electronics & Communication Engg. from Haldia Institute of Technology, Haldia affiliated to West Bengal University of Technology, Kolkata in 2008. Mr. Ojha is a graduate student member of IEEE and student member of ACM. Currently, he is serving as the Chair of the Executive Committee at IEEE Student Branch, IIT Kharagpur. He is also the Organizing Chair of IEEE TechSym 2016 to be held at IIT Kharagpur. He serves as a TPC member for IEEE ScalCom 2014, IEEE TechSym 2014 and ICACIE 2016 and reviewer for several conferences and journals. He was the winner of GE Edison Challenge 2013 with cash prize of INR 10 Lakhs. He is a co-founder of SkinCurate Research.*

***Supervisors: Dr. Sudip Misra, Dr. Narendra Singh Raghuwanshi***

**Architecture and Resource Management for Green Sensor-Cloud Applications**

The sensor-cloud framework refers to the advent of cloud computing for enhanced monitoring of on-field distributed WSNs. This integrated framework empowers the typical WSNs in terms of improved processing power and storage capacity. Sensor-cloud provides efficient data management and access in a WSN deployment spanning a vast geographical area. Also, the sharing of computing resources in a cloud computing framework increases the resource utilization. This facilitates the development of real-time decision support system for use with multiple WSN applications at the same time. Using the principle of virtualization, the sensor-cloud architecture attains complete abstraction of deployed nodes and underlying topology. Typically, the on-field WSNs periodically update the sensed information in the cloud framework. However, frequent update of information increases energy consumption, and at the same time, increases the bandwidth requirement. In resource constrained networks such as WSNs, it is desirable to minimize energy consumption to maximize the sensor lifetime, while maintaining the delay constraint. In this thesis, we propose an architecture for sensor-cloud which can facilitate resource management. Also, we present how dynamic duty scheduling of the sensor nodes can significantly minimize the energy consumption of the on-field WSNs and consequently facilitate resource management.

**Tanwi Mallick**
Email: tanwimallick@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: Partha Pratim Das, Arun Kumar Majumdar***

**Computer analysis of Indian Classical Dance**

The broad goal of my research is Computer analysis of Indian Classical Dance Bharatanatyam. It is an ancient heritage of India, consists of visual, auditory and textual information that tell a story through body movements, hand gestures or hasta-mudras, vocal and instrumental music, facial expression or emotions (nava-rasa)'s, costume, and make-up. With time, these dance forms have been immersed with various sets of complex rules have emerged for body postures and gestures.

My objective is to analyse the multimedia aspects of Bharatanatyam Adavu using Kinect. Analysis of Adavu involves analysis of the component parts like video, audio, and their relations in making up a complete dance. We solve the problem using a three-tier approach. In this approach the lower tier is data acquisition and pre-processing, middle tier is data-driven tier for dance sub-sequence recognition and the upper tier is knowledge-based to support Adavu recognition based on the inherent structure of Bharatanatyam Adavu.

**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.*

***Supervisors: Prof. Sudebkumar Prasant Pal, Prof. Rogers Mattew***

**Bisecting families of hypergraphs**

Let n be any positive integer and F be a family of subsets of [n] = {1,...,n}. Another family F' of subsets of [n] is called a bisecting family for F, if for each subset f in F, there exists a subset f' in F' such that |f \cap f'| is floor(|f|/2), or ceil(|f|/2). Let \beta(F) denote the minimum cardinality of a bisecting family for F. We define \beta(n) as the maximum of \beta(F) over all families F on [n]. We study the problem of computation/estimation of \beta(F) and \beta(n).

**Application**:
Given an bicoloring B, an path {v_1,...,v_k} is said to be alternating if any pair of consecutive vertices are colored with different colors. Consider a two player game consisting of an adversery A and a player P. A first chooses a natural number n. Then, P has to generate a set of bicolorings C={B_1,...} of n vertices.
Now, A gives any set f consisting of even number of vertices. Player P wins if given f as input, P has a bicoloring in C where there is an alternating path consisting of only the vertices of f. The minimum cardinality of C that P has to choose in order to win is equal to \beta(n).

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

*I am a PhD student in the Department of Computer Science and Engineering, IIT Kharagpur, since January 2015. My Ph.D. is jointly advised by Dr. Rajat Subhra Chakraborty and Dr. Debdeep Mukhopadhyay. I am interested in Hardware Security and actively involved in implementation of Physically Unclonable Functions (PUFs) as a hardware security primitive for designing lightweight authentication protocols in the Internet of Things framework. I also have worked on the cryptanalysis of PUFs and efficient software implementation of Cryptographic Pairing for secure communication in different platforms of sensor motes.*

***Supervisors: Dr. Rajat Subhra Chakraborty, Dr. Debdeep Mukhopdhyay***

**Lightweight Authentication Protocols Design for Internet of Things Framework**

The Internet-of-Things (IoT) is an emergent technology focused on enabling widespread connectivity of systems, devices and services. In the IoT, each object is uniquely identifiable through its embedded computing structure, and also inter-operable in the Internet infrastructure. Security is of paramount importance, and carefully designed cryptographic and authentication protocols are required to be

implemented in the resource-constrained IoT setup. My purpose of research is to develop and analyse a lightweight identity-based cryptosystem suitable for resource constrained environments such as IoT, to enable secure authentication and message exchange among the devices. Additionally, to identify the devices uniquely, my work will try to employ Physically Unclonable Function (PUF), to generate the public identity of each device, which is used as the public key for each device for message encryption. The formal proofs of security in the two different attack models, Session Key security and Universally Composable Framework of the protocol will be demonstrated to show the resilience of the scheme against passive as well as active attacks. For implementation purpose, we will deploy our scheme in two different kinds of platforms which are: Intel Edison Board and the CDAC Ubimotes. For implementing the PUFs, we will use the Xilinx Artix 7 FPGA Board. Our work would be directed towards low-overhead hardware/software co-design of the proposed architecture on such IoT testbed, and evaluation of the robustness of the implementation with respect to implementation-specific attacks such as side channel analysis.

# 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 December 2013, he has been a research scholar in the Department of Computer Science & Engineering, IIT Kharagpur. His primary research interests are in the areas of Computer Architecture, Cryptography, and VLSI design.*

***Supervisor: Prof. Debdeep Mukhopadhyay***

### Side-channel Analysis of Shift Register Based Stream Ciphers

Encryption and decryption algorithms are extensively used in embedded systems for secured and authorized data communication between a transmitter and a receiver over an insecure channel. In recent years, side-channel attacks (SCA) have been established to be a very powerful attack against standard cipher designs. In SCA, an adversary exploits the unintentional leakage of information into the environment from a cryptographic device to reveal the secret key. These attacks are possible even on cryptosystems whose theoretical robustness has been well established under various mathematical models and statistical analysis. My current research primarily focusses on side-channel vulnerability assessment of standard stream cipher implementations as proposed in the eSTREAM project.

**Amit Samanta**
Email: amit.samanta049@gmail.com
Joined the department in: December 2013

***Amit Samanta*** *is pursuing MS By Research in Department of Computer Science and Engineering, Indian Institute of Technology Kharagpur. He has completed my B.Tech degree in Electronics and Communication Engineering from West Bengal University of Technology.*

***Supervisor: Dr. Sudip Misra***

### QoS-Aware Resource Provisioning in Wireless Body Area Networks

The constant miniaturization of electronic devices and the development of low-power, invasive/non-invasive, lightweight wireless sensor nodes have triggered an evolution in sensor-based event monitoring systems in varied domains. Wireless Body Area Networks (WBANs), in recent times, have gained popularity in the context of remote, ubiquitous, and seamless monitoring of human physiological parameters contentiously around the clock. Although WBANs provide remote and ubiquitous healthcare services but mobility of limbs, and in turn, the on-body sensor nodes causes the network topology to change periodically. This significantly deteriorates the link-quality between the sensor nodes and the LPU. Also, the group-based mobility of WBANs hampers the communication link between the LPUs and APs considerably. Consequently, the variation in the link-quality unnecessarily depletes the available resources of the sensor nodes and also increases the packet delivery delay. Thus, a need to provide eefficient solutions to these technical challenges is imminent. The main focus of this problem is to improve the data transmission techniques, while minimizing the packet delivery delay and maximizing the throughput of WBANs in the presence of body movements and mobility of WBANs. We also analyze the performance of MAC protocol | IEEE 802.15.6 to provide the reliable communication to WBANs.

**Aniket Roy**
Email: aniketroy@iitkgp.ac.in
Joined the department in: January 2015

***Supervisor: Dr. Rajat Subhra Chakraborty***

*Aniket Roy received his B.Tech degree in Electronics & Communication Engineering from Kalyani Govt. Engg. College in 2014. Since January 2015, he has been a research scholar in the department of Computer Science & Engineering, IIT Kharagpur. His research interests are in the areas of Reversible Image Watermarking and Multimedia Security.*

### Multimedia security through Reversible Watermarking

Digital watermarking is an important technique adopted for copyright protection and authentication. Digital watermarking is the act of hiding secret information (termed a "watermark") into a digital "cover" medium (image, audio or video), such that this information may be extracted later for authentication of the cover. However, the process of watermark embedding in the cover medium usually leads to distortion of the latter, even if it is perceptually negligible. Reversible watermarking is a special class of digital watermarking, whereby after watermark extraction, both the watermark and the cover medium remain unmodified, bit-by-bit. In traditional reversible watermarking schemes, the watermark to be embedded is usually generated as a cryptographic hash of the cover image. The two major factors of a reversible watermarking scheme are embedding capacity (how many watermark bits can be embedded into the image reversibly) and distortion (between the original image and the watermarked image). Reversible watermarking is most widely used in industries dealing with highly sensitive data, such as the military, medical and legal industries, where data integrity is the major concern for users. My current research work investigates the theoretical analysis of several reversible image watermarking algorithms. Moreover, capacity distortion performance improvement for several format of images like color image reversible watermarking is also another direction of research.

**Anirban Ghose**
Email: anighose25@gmail.com
Joined the department in: December 2013

***Anirban Ghose*** *completed his B. Tech in Computer Science and Engineering from Heritage Institute of Technology in 2013 and has been a Research Scholar in the department from December 2013. His primary areas of research interest are High Performance Computer Architecture and Machine Learning.*

***Supervisor: Dr. Soumyajit Dey, Dr. Pabitra Mitra***

### Machine Learning based Heterogeneous Runtime Systems

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. The work in progress also strives to incorporate 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. Future work entails developing a robust Machine Learning based scheduling framework for heterogeneous multicores for execution of multiple OpenCL programs together.

**Arijul Haque**
Email: rjlhq05@gmail.com
Joined the department in: January 2013

M. S.: Pursuing
Broad research topic: Speech processing.
Research area: Emotion conversion in speech.
Research interests: DSP, Machine Learning, Audio Signal Processing.
Publications: Two international conference papers published.

***Supervisor: Krothapalli Sreenivasa Rao***

**Emotion Conversion in Speech**

Given a speech signal in neutral style, the target is to process that signal so as to mimic a target emotion, for example, sadness or anger.

**Debasmita Lohar**
Email: debasmita.lohar@cse.iitkgp.ernet.in
Joined the department in: December 2013

***Debasmita Lohar*** *received a B.Tech. Degree in Computer Science and Engineering from Heritage Institute of Technology, Kolkata, in 2013. From September 2013 to January 2016, she worked 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". From January 2016, she is working as a Research Consultant under the project: "RTOS Validation and Development Support". Her research interests are in the areas of Formal Methods in Software Verification, Program Analysis and Embedded System.*

***Supervisor: Dr. Soumyajit Dey***

**Probabilistic Program Analysis for Software Reliability**

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.

**Gurunath Reddy M**
Email: mgurunathreddy@sit.iitkgp.ernet.in
Joined the department in: January 2012

***Gurunath Reddy M*** *is from Bangalore, India. Pursuing MS (by research) at School of Information Technology, IIT Kharagpur on the thesis titled "Predominant Melody Extraction from Indian Classical Vocal Polyphonic Music Signals ". Parallel to MS, he is working as a Research assistant for developing on-line pedagogical music learning tools for tutoring applications and Children story speech synthesis in Indian Languages. His research interests includes : Music signal processing, Speech processing and Machine Learning.*

***Supervisor: Dr. K Sreenivasa Rao***

**Melody Extraction from Vocal Polyphonic Music Signals**

Melody extraction is the task of automatically extracting the dominant melodic line in a polyphonic music signal. Here, polyphony refers to the music signal in which two or more instruments may sound simultaneously (e.g. voice, tanpura and tabla) or it can be a single instrument which is capable of playing more than one note at a time (e.g. the violin). The term melody is a musicological concept which is based on the judgment of human listeners and we can expect to find different definitions for the melody in different contexts. The melody representation adopted in this work is fundamental frequency (F0) values correspond to the perceived pitch of the dominant instrument. The dominant instrument can be either the human singing voice or the lead instrument in the polyphonic music signal. The accurate extraction of the melody is remained as challenging and unsolved task in the research community because the complexity of the task is two folds. Firstly, the polyphonic music signal contains superposition of all instruments which play simultaneously. Hence, it is hard to attribute specific frequency bands and energy levels to specific instrument. Secondly, the task of determining which pitches constitute the main melody needs to be addressed. This in turn entails three main challenges: (i) determining when the melody is present and when it is not, (ii) ensuring the estimated F0 is in the correct octave and (iii) selecting the correct melody pitch when there is more than one note present at the same time.

**Harikrishna D M**
Email: coolhari2006@gmail.com
Joined the department in: December 2012

***Harikrishna D M*** *received his B.E. degree in Computer Science from Siddaganga Institute of Technology, Tumkur in 2010. After receiving B.E., he worked as software developer in Laurus Infosystems, Bangalore. Since December 2012, he is doing his MS in the school of information technology, IIT Kharagpur. His current research interests are in the areas of Speech and natural language processing.*

***Supervisor: K. Sreenivasa Rao***

## Multi-stage Children Story Speech Synthesis

Story speech synthesis aims at synthesizing story-style speech from the text using text-to-speech (TTS) systems. Synthesizing expressive speech involves embedding natural expressions into speech, according to the semantics present in the text. Generating an expressive, naturally sounding, story like speech from text using a neutral TTS system is a highly challenging task. We have attempted this task by dividing it into multiple stages such as: (i) identifying whether the given text is related to story or not, (ii) identifying the story genre from the story text, (iii) identifying emotions specific to story genres, (iv) deriving prosody modification factors (rules) for story specific emotions and (v) synthesizing the story style speech from neutral TTS by incorporating the derived prosody modification factors.

**K Sai Ram**
Email: sairam.kasanagottu@gmail.com
Joined the department in: December 2014

***K Sai Ram*** *is an MS student in the Department of Computer Science and Engineering, IIT Kharagpur, since Dec 2014 under the joint guidance of Prof. Jayanta Mukhopadhyay and Prof. Partha Pratim Das. He graduated from Indian Institute of Technology, in the department of Electronics and Electrical Communication Engineering, and then worked in Philips India Private Limited, Noida, India, as Assistant Manager in LED Development Labs. His research interests are in the areas of Robotics, Computer Vision, Image Processing and Pattern Recognition.*

***Supervisor: Prof. Jayanta Mukhopadhyay, Prof. Partha Pratim Das***

## Design autonomous aerial vehicles to navigate in unknown outdoor and indoor environments

The aim of this project is to create an autonomous quadrotor, capable of balancing itself, and will be capable of stable flight. It will also be able to track moving robots on the ground and interact with them in a new innovative way. It will be self-aware and able to navigate autonomously in a own environment. Develop an autonomous unmanned aerial vehicle which is aware of its surroundings and capable of navigating in indoor and outdoor environments. It would be useful in several applications in the fields of surveillance, 3D environment mapping and further applications which can be achieved using a team of such robots.

**Malay Pramanick**
Email: malaypramanick15@gmail.com
Joined the department in: March 2015

***Malay Pramanick*** *graduated in 2014, from the Department of Computer Science and Engineering. After receiving his B.Tech, he joined Abzooba Infotech as a Research Associate. He left Abzooba to join IIT Kharagpur in 2015, to pursue academic research, as a Junior Research Fellow. His primary research interests are in Natural Language Processing, Cognitive Science, Machine Learning and Artificial Intelligence.*

***Supervisor: Pabitra Mitra***

## Multi-Objective Optimization

Malay Pramanick works on support system optimization with various optimization techniques. With Pareto optimization being the mostly exerted on optimization problem.

**Paheli Bhattacharya**
Email: paheli@iitkgp.ac.in
Joined the department in: July 2014

***Paheli Bhattacharya*** *is a Master of Science (MS, by Research) student in the Department of Computer Science and Engineering at IIT Kharagpur. She completed her BTech from Government College of Engineering and Textile Technology, Semaphore (WBUT). Her areas of interest include Natural Language Processing, Information Retrieval and Machine Learning.*

***Supervisor: Prof. Pawan Goyal, Prof. Sudeshna Sarkar***

**Improving Cross Lingual Word Embeddings for Indian Languages**

I am currently working on improving vector space representation of words in Indian languages, that can help in Machine Translation, Cross-Language Information Access and expanding the low amount of resources we have for Indian languages (for example, inducing bilingual lexicons)

**Pallavi Mitra**
Email: pallavi.mitra1992@gmail.com
Joined the department in: May 2015

***Supervisor: Dr. Soumyajit Dey***

***Pallavi Mitra*** *is currently pursuing Master of Science(By Research) from the Department of Computer Science and Engineering, Indian Institute of Technology,Kharagpur, India under the supervision of Dr. Soumyajit Dey and Dr. Pabitra Mitra. She has completed her B.E in Electronics and Telecommunication Engineering from Jadavpur University.*

**Speech Processing in GPGPU platforms.**

Problem Description - I am working in "Architectural and Algorithmic Optimizations for Speech Based Communication Interface on Mobile Device" . We plan to develop an Recurrent Neural Network based End to End Automatic Speech Recognition System for a Windows based embedded platform comprising an integrated Intel CPU and GPU.

**Parakrant Sarkar**
Email: parakrantsarkar@gmail.com
Joined the department in: December 2012

***Parakrant Sarkar*** *is a student at IIT Kharagpur, India pursuing Masters (by research) program.*

***Supervisor: Dr. Krothapalli Sreenivasa Rao***

**Storytelling style Speech Synthesis**

My area of research deals with speech synthesis form machines i.e. Text to speech systems. As a part of

my MS thesis, my objective is on developing a Text to speech system (TTS) that can read children stories as a human reader. In this context we have to use the existing Neutral TTS in order to produce a storytelling style speech. A proper text analysis as well as speech signals analysis is required. This involves succinct analysis of various prosodic aspects like pitch, duration, intensity, prominence, tempo, pause patterns. These parameters are modeled by using machine learning techniques and are incorporated in the neutral speech by using signal processing techniques to convert it into storytelling style speech.

**Rijula Kar**
Email: rijula.cse@iitkgp.ac.in
Joined the department in: July 2015

***Rijula Kar*** *is pursuing M.S in the department of CSE in IIT,Kharagpur. Her broad area of research is Machine Learning. She has received B.E degree from IIEST,Shibpur in 2015.*

***Supervisor: Sourangshu Bhattacharya***

**Collective classification of rumors spreaded in Social Media**

A rumor is defined as an unverified or unconfirmed statement or report circulating in a community. These rumors are created either intentionally or unintentionally, but carry false or even malicious information and spread widely via social media. We have seen that after a disaster event a rumor propagates very fast. So,it is very important to detect rumor and to stop its spreading as soon as possible. Collective classification refers to the combined classification of a set of interlinked objects. We are collectively classifying the rumors and the users spreading the rumors.

**Saptarshi Misra**
Email: saptarshimisra2011@gmail.com
Joined the department in: July, 2015

*Passed B.Tech from Kalyani Government Engineering College with CGPA 8.58 and rank within top 10 in the class. Did schooling from South Point HIgh School. Ranked 26th in the Higher Secondary Examination for which I received National Merit Scholarship by MHRD during B.Tech. Ranked 34th in the 10th examination.Was previously a Microsoft Student Associate and have short-term internship/project experiences ai ISI Kolkata, Vodafone India Pvt. Ltd., Gail India Pvt. Ltd.,etc. Was part of the founding group for a coding club at college. Hobbies: Listening to and singing songs.*

***Supervisors: Prof. Sudeshna Sarkar, Prof. Pabitra Mitra.***

**Feature extraction and analysis of climate data using data mining techniques**

Climatic events are very complex phenomena involving high level of spatio-temporal variations and prediction of climate including rainfall,temperature,etc. is very essential for agriculture-dependent countries like India. Presently, I am working on a problem of statistical downscaling of global climate models to predict the rainfall of a small region such as Mahanadi basin. The global climate models when projected on a local scale does not give acceptable results and fail to model the spatio-temporal variations,specially variables like rainfall having huge variations location wise and day-wise. For this, we plan to use some deep learning model like a stacked autoencoder to perform the task of statistical downscaling to predict future rainfall/future climate over a small region such as Mahanadi basin. Based on the present performance of various deep learning models in predicting various complex

phenomena even involving spatio-temporal variations, we believe that they will give much better results in predicting rainfall/climate using statistical downscaling mechanism.

**Saptarshi Pal**
Email: pal.saptarshi@iitkgp.ac.in
Joined the department in: June, 2015

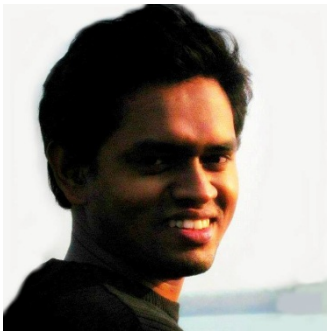
*He has received Bachelor of Engineering from Indian Institute of Engineering Science and Technology, Shibpur (IIEST Shibpur)*

***Supervisors: Prof. Soumya K. Ghosh***

**Prediction in spatio temporal data**

With the advent of remote sensing technologies, there is a lot of data which has spatial and temporal context. For example, USGS provides landsat images so that analysis can be done on it. Satellite images produces a lot of useful information as climate, built-up, landuse etc. My current work is based on prediction of these parameters from satellite data using machine learning techniques

**Sankarshan Mridha**
Email: sankarshan@iitkgp.ac.in
Joined the department in: October 2014



***Sankarshan Mridha*** *completed his B.E in Computer Science and Engineering from Jadavpur University in 2013. He is currently pursuing MS in Computer Science from IIT Kharagpur. His broad area of research is Complex Network and Machine Learning.*

***Supervisor: Prof. Sourangshu Bhattacharya, Prof. Niloy Ganguly***

**Understanding Uncertainty travel time estimation**

Accurate estimation of urban link travel times is essential for traffic operators and travellers, not only because link travel time is an important index for monitoring and evaluating the state of the traffic on an urban road network, but also because it is a critical input to dynamic route guidance systems which helps travellers make better route choices and avoid congestion. The estimation of urban link travel times relies on traffic data collection. In the past, traffic data were mainly collected by loop detectors. However, due to the high cost of installation and maintenance, loop detectors are often only installed on a few links in the urban road network, which leads to unavailability of most of the network traffic data. In recent years, most vehicles are equipped with GPS devices such as GPS navigators or smartphones, which provide a type of probe vehicle which can collect traffic data from the entire road network at low cost. These GPS probe vehicles can continuously collect traffic data by travelling on the road. Now The aim of this project is to propose a citywide model for estimating the travel time of any path (represented as a sequence of connected road segments) in a city using partial information obtained from large scale yellow cab GPS data from New York City over a period of one year. The idea here is to infer the road network from the partial data followed by estimation of the link travel time and capture the uncertainty to provide a better service to the city commuters.

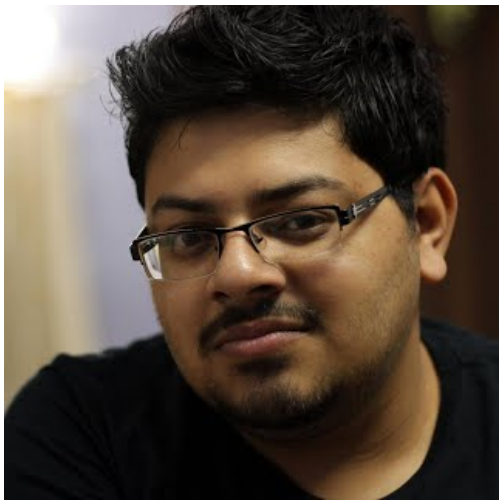
**Sanku Kumar Roy**
Email: sankukumarroy@gmail.com
Joined the department in: January, 2015

*I am currently pursuing Master of Science (By Research) from the Department of Computer Science and Engineering, Indian Institute of Technology Kharagpur, India under the supervision of Dr. Sudip Misra and Dr. Narendra Singh Raghuwanshi. Also, I am working as a Junior Research Fellow in "Development of a Sensor based Networking System for Improved Water Management for Irrigated Crops" funded by MHRD, Government of India. I completed bachelor of technology in Electronics & Communication Engineering from West Bengal University of Technology.*

***Supervisors: Dr. Sudip Misra, Dr. Narendra Singh Raghuwanshi***

**Interoperability in Internet of Things**

Internet of things (IoT) is a dynamic global infrastructure, in which physical objects can interact with any other physical objects, and share their information. Any device can communicate with any other devices anytime from anywhere. But, there are heterogeneous things, heterogeneous protocols, and heterogeneous communication networks. To develop an IoT network, we have to solve the heterogeneity of things, protocols, and networks.



**Satadal Sengupta**
Email: satadal.sengupta.nit@gmail.com
Joined the department in: January, 2016

*Satadal is a 1st year MS Student since January, 2016 and a Junior Research Fellow in the Department of Computer Science and Engineering at Indian Institute of Technology Kharagpur, India. He works with Dr. Sandip Chakraborty and Prof. Niloy Ganguly. His research interests lie in the fields of Mobile Computing and Wireless Networks. Satadal completed his Bachelor of Technology in Computer Science and Engineering from National Institute of Technology Durgapur, India in 2013. He worked as an Associate Applications Developer in Oracle Financial Services Software Ltd., Bangalore, India from September, 2013 to April, 2015. He has also worked with Microsoft IT, Hyderabad, India as a Software Development Engineer (SDE) during his summer internship from May to July, 2012.*

***Supervisors: Prof Sandip Chakraborty, Prof. Niloy Ganguly***

**Measurement and Analysis of Differential Pricing of Internet Services in Developing Countries**

Internet access is one of the most enabling factors in today's world. It opens the door to terabytes and petabytes of digital information - produced, archived and consumed by the world population. This access is limited in developing countries, which however have a booming penetration of mobile phones and similar hand-held devices. These devices have hardware and software capable for Internet access, but might not have actual access for lack of a paid data connection from a cellular provider. To harness the ubiquity of end-user mobile devices and introduce more people to the Internet, there have been some recent efforts of differential pricing of Internet services in developing countries. Facebook's Internet.org or FreeBasics is one such differential pricing program, which is the primary focus of this research.

Differential pricing of Internet services in general and FreeBasics in particular is creating tremendous debates in the developing countries. There is significant polarization of opinions about the positives and negatives of such a program. Most of these debates have been qualitative in the form of comments and arguments in the social networks and blog posts. The main aim of this research is to add some

quantitative data to these debates through careful experimentation, measurement and analysis.

**Shiladitya Ghosh**
Email: Shiladitya.ghosh@cse.iitkgp.ernet.in
Joined the department in: January 2014

*Shiladitya Ghosh received his B.Tech. in Computer Science and Engg. 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 IndianInstitute 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.*

***Supervisor: Prof. Pallab Dasgupta, Prof. Chittaranjan Mandal***

**Formal Modeling and Validation of Railway Interlocking and Train Control Systems**

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 verifies 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).

**Subhendu Khatuya**
Email: subha.cse143@gmail.com
Joined the department in: June 2015

***Subhendu Khatuya*** *received his B.Tech degree from Kalyani Govt. Engg. College in CSE in 2014. Currently he is doing his M.S in Computer Science from IIT Kharagpur.*

***Supervisor: Dr. Bivas Mitra, Dr. Niloy Ganguly***

**EMS Log Analytics for Anomaly Detection**

Predicting the system anomaly as early as possible.

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

***Sulagna Gope*** *is presently pursuing MS in dept. of Computer Science and Engineering, IIT Kharagpur. She did her B.Tech from Heritage Institute of Technology(WBUT), Kolkata.*

***Supervisor: Prof. Sudeshna Sarkar, Prof Pabitra Mitra***

## Weather prediction using Machine Learning techniques

Climate modelling is an extremely difficult task as it involves a huge range of parameters. The traditional models are mainly physics based that require a lot of manual intervention for designing. We want to automate the process by using a datacentric approach of model training and learning. For this purpose we are using the latest techniques in machine learning.

# 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 Technology Kharagpur. He received his M.Tech. and Ph.D. degrees from the Institute of Radio Physics and Electronics, Calcutta University 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*

Presently, Animesh Mukherjee is an Associate Professor in the Department of Computer Science and Engineering, Indian Institute of Technology Kharagpur. Prior to this, he worked as an Assistant Professor in the same Department for the last four and a half years. Immediately before that he was a post-doctoral researcher in the Complex Systems Lagrange Lab, ISI Foundation, Italy. He received his PhD from the Department of Computer Science and Engineering, Indian Institute of Technology Kharagpur with a thesis on "self-organization of human speech sound inventories". His main research interests center around applying complex system approaches (mainly complex networks and agent-based simulations) to different problems in

(a) Human language evolution and change,

(b) Web social media,
(c) Information retrieval, and
(d) Natural language processing

He has received many notable awards including the INAE Young Engineer Award 2012, INSA Medal for Young Scientists 2014 and the IBM Faculty Award 2015. He has authored more than 60 articles in top-tier CS conferences and high impact journals.

**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.

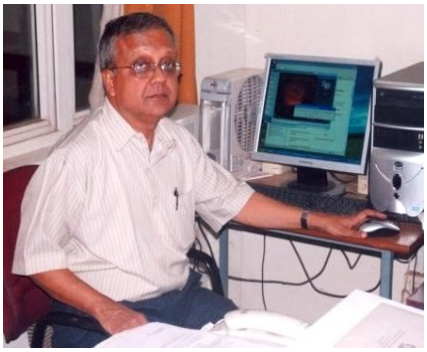
He has won several awards and honors for his research contributions. These include the National Award for the Best Technology Innovation for the Physically Disabled (2007), the Da Vinci Award 2004, and Outstanding Young Person Award 1996.

**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 from the University of Alabama in 1992, and an M.E. and a B.E. in Electronics and Telecommunication Engineering from Jadavpur University, Kolkata, India in 1990 and 1987 respectively. From February 199 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 Department of Computer Science & Engineering at IIT Kharagpur, India. He earned his Ph.D in Computer Science & 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.

**Debasis Samanta**
Email: dsamanta@sit.iitkgp.ernet.in

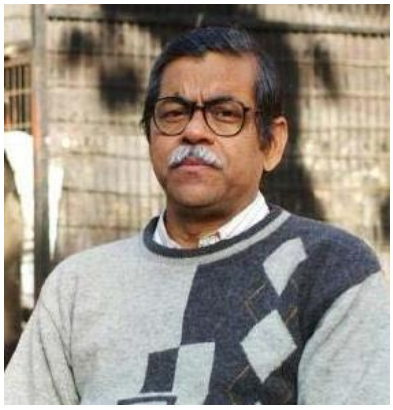
**Research Interest:** *Augmentative and Alternative Communication Systems, Human Computer Interaction, Model-Based Testing, Cognitive Science, Biometrics*

Debasis Samanta received his Ph.D from Indian Institute of Technology Kharagpur, M.Tech. from Jadavpur University, and B.Tech. from Calcutta University. Before joining IIT Kharagpur in 2004, he was a Senior Lecturer in North Eastern Regional Institute of Science and Technology (NERIST), Itanagar. His research includes logic synthesis for low power high performance VLSI CMOS circuits, models and algorithms for design of scanning keyboards, automatic synthesis of test cases with some UML behavioural models, test coverage analysis of object-oriented programs, multimodal biometric authentication systems, integration testing of object-oriented systems using UML, and multimodal user interface to Internet for common people. He is a senior member of IEEE since 1999 and the Chair of IEEE Kharagpur Section during 2009-2010.

**Debdeep Mukhopadhyay**
Email: debdeep@cse.iitkgp.ernet.in

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

Dr. Debdeep Mukhopadhyay is currently an Associate Professor at the Department of Computer Science and Engineering, Indian Institute of Technology at Kharagpur, India. At IIT Kharagpur he initiated the Secured Embedded Architecture Laboratory (SEAL), with a focus on Embedded Security and Side Channel Attacks (http://cse.iitkgp.ac.in/resgrp/seal/). Prior to this he worked as a visiting Associate Professor of NYU-Shanghai. He had also served as an Assistant Professor at IIT Madras, India and as a Visiting Researcher at NYU Polytechnic School of Engineering under the Indo-US STF Fellowship. He holds a PhD, an MS, and a B. Tech from IIT Kharagpur, India. Dr. Mukhopadhyay's research interests are Cryptography, Hardware Security, and VLSI. His books include Cryptography and Network Security (Mc Graw Hills), Hardware Security: Design, Threats, and Safeguards (CRC Press), and Timing Channels in Cryptography (Springer). He has written more than 100 papers in peer-reviewed conferences and journals and has collaborated with several Indian and Foreign Organizations. Dr. Mukhopadhyay is the recipient of the prestigious Young Scientist award from the Indian National Science Academy, the Young Engineer award from the Indian National Academy of Engineers, and is the Young Associate of the Indian Academy of Science. He was also awarded the Outstanding Young Faculty fellowship in 2011 from IIT Kharagpur, and the Techno-Inventor Best PhD award by the Indian Semiconductor Association. He has recently incubated a start-up on Hardware Security, ESP Pvt Ltd at IIT Kharagpur (http://esp-research.com/).



**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 a 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).

**Goutam Biswas**
Email: goutam@cse.iitkgp.ernet.in

***Research Interests:*** *Theoretical computer science, compilers*

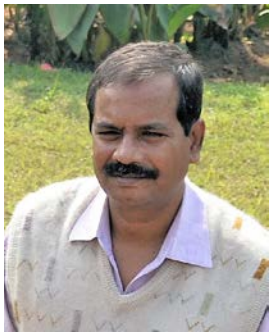
**Indranil Sengupta**
Email: isg@cse.iitkgp.ernet.in

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

Dr. Indranil Sengupta obtained his B.Tech., M.Tech. and Ph.D. degrees 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).

**Krothapalli Sreenivasa Rao**
Email: ksrao@sit.iitkgp.ernet.in

**Research Interest:** *Speech Processing, Image Processing, Multimedia Signal Processing, VLSI and Signal Processing*

K. Sreenivasa Rao obtained his PhD from IIT Madras in 2005, M.E (Comm. Sys.) from PSG Tech., Coimbatore in 1993, and B.Tech (ECE) from Nagarjuna University, Guntur, in 1990. Before joining IIT Kharagpur in 2007, he held faculty positions in IIT Guwahati and Baptala Engineering College, and was a project officer in IIT Madras. Dr. Rao started the activity of speech processing in the School of Information Technology, since 2007. The basic objectives of his group are: (1) Development of speech systems in Indian languages, (2) Characterization and incorporation of natural emotions in speech systems, (3) Development of speech systems for mobile devices and (4) Screen readers in Indian languages applicable to visually challenged people. Dr. Rao has about one hundred publications as book chapters and papers in reputed journals and conferences.

**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 and is currently a Professor at the Dept. of Computer Sc. & Engg. His research interests include Formal Verification, Artificial Intelligence and VLSI. He has over 160 research papers and 3 books in these areas. The Formal Methods Group (http://cse.iitkgp.ac.in/~pallab) under his leadership works in the validation of integrated circuits, cyber-physical systems, railway signalling, smart grids, and safety critical software in collaboration with several companies, including Intel, Synopsys, General Motors, SRC, Indian Railways and Hindustan Aeronautics . Dr. Dasgupta has been a recipient of the Young Scientist awards from the Indian National Science Academy (INSA), Indian National Academy of Engineering (INAE), and the Indian Academy of Science (IASc). He is a Fellow of INAE, Fellow of IASc, and Fellow of IETE. Dr. Dasgupta serves as an Associate Editor of the IEEE Transactions on Computer Aided Design of Integrated Circuits and Systems. Presently he holds the additional 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:*** *Image processing and computer vision, technology-enabled education, 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 the Dept 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 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 Co-General Chair for International Conference on VLSI Design & Embedded Systems in 2005, and as Co-Program-Chair in 2016 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 Surveys.

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), Technology-enabled Education (Digital Library and Distance Education), 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 Associate Professor in the Computer Science and Engineering Department of Indian Instutute of Technology Kharagpur. He has a Ph.D. in Computer Engineering from Case Western Reserve University and a B.E. (Hons.) in Electronics and Telecommunication Engineering from Jadavpur University (India) in 2005. He has work experience at National Semiconductor and AMD. His research interests include: Hardware Security, VLSI Design and Design Authomation, and Reversible Watermarking for digital content protection. He is the co-author of three published books five book chapters, and close to 70 publications in international journals and conferences of repute. His work has been cited close to 1200 times. He is one of the recipients of the "IBM Faculty Award" for 2012, and a "Royal Academy of Engineering (U.K.) Fellowship" in 2014. He holds 1 U.S. patent, and 2 more international patents and 3 Indian patents have been filed based on his research work. Dr. Chakraborty is a member of IEEE and ACM.

**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.

## Rajiv Ranjan Sahay

***Research interests:*** *Image Processing, Computer Vision, Multimedia*

Rajiv Ranjan Sahay obtained his PhD from IIT Madras. He was a post-doctoral fellow at the School of Computing, National University of Singapore (NUS). He joined the School of Information Technology of IIT Kharagpur in 2012. Currently, he is an Assistant Professor in the Department of Electrical Engineering of IIT Kharagpur. He is a member of IEEE. He has more than 20 research papers and a patent on recovering 3D structure using blur and parallax.

## Rogers Mathew

***Research interests:*** *Graph Theory, Combinatorics, Graph Algorithms*

Rogers Mathew obtained his PhD and ME (CSE) from Indian Institute of Science Bangalore in 2012 and 2007, and BTech (CSE) from College of Engineering, Trivandrum in 2003. Before joining IIT Kharagpur in 2015, he held post-doctoral positions in University of Haifa, Israel and Dalhousie University, Halifax, Canada. He also worked as a Software Engineer in Infosys Technologies, Bangalore. His teaching and research focus on combinatorics, graph theory, and graph algorithms. He has about 20 publications in reputed journals and conferences.

## Sandip Chakraborty

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

Sandip Chakraborty obtained his PhD and MTech in Computer Science from Indian Institute of Technology, Guwahati in 2014 and 2011, and BE in Information Technology from Jadavpur University in 2009. Before joining IIT Kharagpur in 2014, he held positions of postdoctoral fellow, project fellow and visiting assistant professor in IIT Guwahati. He has bagged many awards for his research and academic activities.

The research interest of Sandip spans the domain of wireless networks, mobile computing and distributed computing. He is particularly interested in system development for communication, ranging from broadband wireless to smart city communication. We are living in the era of small handheld devices where wireless communication is a primary requirement.

The major problem in wireless communication is that everything is open to all. Consider you are talking in a free space. Everyone around you can hear the message. This imposes immense challenges when a group of people wants to talk with each other. If everyone starts talking simultaneously, it results in a big noise, and no one can understand what the other is talking about. Further, think if you want to share some secret messages, what can be the scenario! Remember, you can only talk and nothing else! So this is the scenario for wireless communication. There are several open challenges that require system-level engineering. Sandip loves to travel in this research space.

**Shamik Sural**
Email: shamik@sit.iitkgp.ernet.in

Shamik Sural is a professor at the Computer Science and Engineering Department, IIT Kharagpur. He received the Ph.D. degree from Jadavpur University. He is a recipient of the Alexander von Humboldt Fellowship for Experienced Researchers. Shamik has published more than 150 research papers. His research interests include computer security, data mining and database systems.

**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.

**Soumya Kanti Ghosh**
Email: skg@sit.iitkgp.ernet.in

***Research Interests****: Geospatial Science, Network, Cloud Computing, Cloud Security*

Soumya Kanti Ghosh is a Professor in the School of Information Technology, Indian Institute of Technology, Kharagpur (IIT Kharagpur), India. His primary areas of research include Geospatial Databases and Services, Cloud Computing, and Security. Prior to IIT Kharagpur, he worked for Indian Space Research Organization in the area of remote sensing and geographic Information systems for natural resource management. He did his PhD and MTech in Computer Science, from the Department of Computer Science and Engineering, IIT Kharagpur. He did his BE in Electronics and Communication Engineering from National Institute of Technology (formerly, Regional Engineering College), Durgapur, India.

**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 is also working on applications of Artificial Intelligence in Climate Mining and in Transportation and Logistics.

**Sudip Misra**
Email: smisra@sit.iitkgp.ernet.in

**Research Interest:** *Wireless Sensor Networks, Cloud Computing, Big Data Networking, Software Defined Networking, Internet of Things, Smart Grid, Delay Tolerant Networks, Nano-Sensor Networks*

Dr. Sudip Misra is an Associate Professor in the Department of Computer Science and Engineering at the Indian Institute of Technology Kharagpur. Prior to this he was associated with Cornell University (USA), Yale University (USA), Nortel Networks (Canada) and the Government of Ontario (Canada). He received his Ph.D. degree in Computer Science from Carleton University, in Ottawa, Canada. He has several years of experience working in the academia, government, and the private sectors in research, teaching, consulting, project management, architecture, software design and product engineering roles.

His current research interests include Wireless Ad Hoc and Sensor Networks, Internet of Things (IoT), Computer Networks, Learning Systems, and algorithm design for emerging communication networks. Dr. Misra is the author of over 260 scholarly research papers, including 140+ reputed journal papers. He has won seven research paper awards in different conferences. Recently, he and his students won Samsung Innovation Award and the IEEE ComSoc Student Competition. He was also awarded the IEEE ComSoc Asia Pacific Outstanding Young Researcher Award at IEEE GLOBECOM 2012, Anaheim, California, USA. He was also the recipient of several academic awards and fellowships such as the Young Scientist Award (National Academy of Sciences, India), Young Systems Scientist Award (Systems Society of India), Young Engineers Award (Institution of Engineers, India), (Canadian) Governor General's Academic Gold Medal at Carleton University, the University Outstanding Graduate Student Award in the Doctoral level at Carleton University and the National Academy of Sciences, India - Swarna Jayanti Puraskar (Golden Jubilee Award).

Dr. Misra was also awarded the Canadian Government's prestigious NSERC Post-Doctoral Fellowship and the Humboldt Research Fellowship in Germany. Dr. Misra has been serving the editorial boards of distinguished journals such as the International Journal of Communication Systems (Wiley) and the IET Wireless Sensor Systems (UK). In the past, he served as the Associate Editor/Editorial Board Member of the IEEE Transactions on Mobile Computing , Telecommunication Systems Journal (Springer), Security and Communication Networks Journal (Wiley), and the EURASIP Journal of Wireless Communications and Networking, IET Communications Journal, and the Computers and Electrical Engineering Journal (Elsevier).

Dr. Misra has published 9 books in the areas of wireless ad hoc networks, wireless sensor networks, wireless mesh networks, communication networks and distributed systems, network reliability and fault tolerance, and information and coding theory, published by reputed publishers such as Cambridge University Press, Springer, Wiley, and World Scientific.

Dr. Misra was invited to chair several international conference/workshop programs and sessions. He served in the program committees of several international conferences. He was also invited to deliver keynote/invited lectures in over 30 international conferences in USA, Canada, Europe, Asia and Africa.

**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 (2015 – 2016)

1. Gaurang Panchal, Debasis Samanta, “Comparable Features and Same Cryptography Key Generation using Biometric Fingerprint Image", 2nd IEEE International Conference on Advances in Electrical, Electronics, Information, Communication and BioInformatics (AEEICB), 2016.

2. Gaurang Panchal, Debasis Samanta, Subhas Barman, “Convolution Code based Unique and Revocable Identity Generation using Fingerprint Image", International Journal of Biometrics and Bioinformatics (IJBB) (Accepted).

3. Gaurang Panchal, Debasis Samanta, “Digital Document Protection System", Indian Patent (2477/ASA/PP-1900/IITKgp), Submitted in October 2015.

4. Sanku Kumar Roy, A. Roy, S. Misra, N. S. Raghuwanshi, and M.S. Obaidat “AID: A Prototype for Agricultural Intrusion Detection Using Wireless Sensor Network”, in ICC, London, UK, 8-12 June 2015, pp. 7059 – 7064.

5. Debashis Mukherjee, Rajib Mall, "An Investigation into Effective Test Coverage", Chapter Advanced Computing and Systems for Security, Volume 396 of the series Advances in Intelligent Systems and Computing pp. 93-106.

6. Mondal, S. Misra, and Mohammad S. Obaidat, "Distributed Home Energy Management System with Storage in Smart Grid Using Game Theory", IEEE Systems Journal, Published on May 22, 2015, DOI: 10.1109/JSYST.2015.2421941.

7. Mondal and S. Misra, "Game-Theoretic Energy Trading Network Topology Control for Electric Vehicles in Mobile Smart Grid", IET Networks, vol. 4, no. 4, pp. 220-228, July 2015.

8. Mondal and S. Misra, "Game-theoretic Green Electric Vehicle Energy Networks Management in Smart Grid", in Proceedings of the IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), Kolkata, India, December 2015 (Accepted).

9. M. P. Singh, S. Sural, V. Atluri, J. Vaidya, and U. Yakub, “Managing multi-dimensional multi-granular security policies using data warehousing”, in Proceedings of the 9th International Conference on Network and System Security, pages 221-235, November 2015.

10. Sankaraganesh Jonna, Vikram S. Voleti, Rajiv R. Sahay and Mohan S. Kankanhalli, “A Multimodal Approach for Image De-fencing and Depth Inpainting”, International Conference on Advances in Pattern Recognition (ICAPR), Kolkata 2015.

11. Sankaraganesh Jonna, Krishna Kanth and Rajiv R. Sahay, “Towards an Automated Image De-fencing Algorithm Using Sparsity”, 10th International Conference on Computer Vision Theory and Applications, VISAPP, Berlin, Germany, 2015.

12. J. Sankarganesh, Krishna Kanth and Rajiv R. Sahay, “My camera can see through fences: A deep learning approach for image de-fencing”, Asian Conference of Pattern Recognition (ACPR), Kuala Lumpur, 2015.

13. Sankarganesh Jonna, Krishna K. Nakka, Vrushali Khasare, Rajiv R. Sahay and Mohan S. Kankanhalli, “Detection and removal of fence occlusions in an image using a video of the static/dynamic scene”, in Journal of Optical Society of America A (JOSA A) (Accepted).

14. Gurunath Reddy M and K. Sreenivasa Rao, "Predominant Melody Extraction from Vocal Polyphonic Music Signal", in 41st IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Shanghai, 2016.

15. Gurunath Reddy M and K. Sreenivasa Rao, "Neutral to Happy Emotion Conversion by Blending Prosody and Laughter", in Eighth IEEE International Conference on Contemporary Computing (IC3), Noida, 2015.

16. Gurunath Reddy M, Procheta Sen, Manjunath K E, Arup Dutta, Arijul Haque, Parakrant Sarkar, K Sreenivasa Rao, "Automatic Pitch Accent Contour Transcription for Indian Languages", in IEEE International Conference on Computer Communication and Control (IC4), 2015.

17. S. Misra, S. Goswami, C. Taneja, A. Mukherjee, Mohammad Obaidat, "A PKI AdaptedModel for Secure Information Dissemination in Industrial Control and Automation", IEEE ACCESS, vol.3, no., pp. 875, 889, 2015 DOI: 10.1109/ACCESS.2015.2445817.

18. Tanmoy Chakraborty, Amrith Krishna, Mayank Singh, Pawan Goyal, Niloy Ganguly, Animesh Mukherjee, "FeRoSA: A faceted recommendation system for scientific articles", in 20th Pacific Asia Conference on Knowledge Discovery and Data Mining (PAKDD), Auckland, New Zealand, April 19-22, 2016 (Accepted).

19. Mayank Singh, Vikas Patidar, Suhansanu Kumar, Tanmoy Chakraborty, Animesh Mukherjee, Pawan Goyal, "The role of citation context in predicting long-term citation profiles: an experimental study based on a massive bibliographic text dataset", in 24th ACM International Conference on Information and Knowledge Management (CIKM 2015), Melbourne, Australia, October 19-23, 2015 (Accepted).

20. Mayank Singh, Tanmoy Chakraborty, Pawan Goyal and Animesh Mukherjee, "ConfAssist: A Conflict resolution framework for assisting the categorization of Computer Science conferences", in Joint Conference on Digital Libraries (JCDL 2015), Tennessee, USA, June 21 -25, 2015 (Accepted).

21. Mayank Singh, Soumajit Pramanik, Tanmoy Chakraborty, "PubIndia: A Framework for Analyzing Indian Research Publications in Computer Sciences", Workshop on Mining Scientific Publications (WOSP), Joint Conference on Digital Libraries (JCDL 2015), Tennessee, USA, June 21 -25, 2015 (Accepted).

22. Pritam Bhattacharya, Subir Kumar Ghosh, and Bodhayan Roy, "Approximability of Guarding Weak Visibility Polygons", Discrete Applied Maths (CALDAM 2015 special issue) (To appear).

23. Pritam Bhattacharya, Subir Kumar Ghosh, and Bodhayan Roy, "Vertex Guarding in Weak Visibility Polygons", in CALDAM 2015, Lecture Notes in Computer Science (LNCS) 8959, pp: 45–57, Springer, 2015 (Received Springer Best Student Paper Award).

24. Samanta, S. Bera, S. Misra, "Link Quality-Aware Resource Allocation with Load Balance in Wireless Body Area Networks", IEEE Systems Journal, 2015.

25. S. Misra, S. Bera, T. Ojha, L. Zhou, "ENTICE: Agent-Based Energy Trading with Incomplete Information in the Smart Grid", Journal of Network and Computer Applications (Elsevier), Vol. 55, pp. 202 - 212, Sept. 2015.

26. S. Bera, S. Misra, and Joel. J. P. C. Rodrigues, "Cloud Computing Applications for Smart Grid: A Survey", IEEE Transactions on Parallel and Distributed Systems, Vol. 26, No. 5, pp. 1477-1494, May 2015.

27. S. Bera, P. Gupta, and S. Misra, "D2S: Dynamic Demand Scheduling in Smart Grid Using Optimal Portfolio Selection Strategy", IEEE Transactions on Smart Grid, Vol. 6, No. 3, pp. 1434-1442, Apr. 2015.

28. S. Misra, S. Bera, and T. Ojha, "D2P: Distributed Dynamic Pricing Policy in Smart Grid for PHEVs Management", IEEE Transactions on Parallel and Distributed Systems, Vol. 26, No. 3,pp. 702-712, Feb. 2015.

29. S. Misra, S. Bera, and M. S. Obaidat, "Economics of Customer's Decisions in Smart Grid", IET Networks, Vol. 4, No. 1, pp. 37-43, Jan. 2015.

30. S. Bera, T. Ojha, S. Misra, and M. S. Obaidat, "Cloud-based Optimal Energy Forecasting for Enabling Green Smart Grid Communication", in Proc. of the IEEE Global Communications Conference (GLOBECOM), 2015.

31. S. Misra, A. Roy, P. Kar, S. Goswami, T. Ojha, "An Adverse Environmental Effect Resistant Seamless Wireless Sensor Network System", Indian Patent Filed, File No. 425/KOL/2015, April 17, 2015.

32. T. Ojha, S. Misra, N. S. Raghuwanshi, "Wireless Sensor Networks for Agriculture: The State-of-the-Art in Practice and Future Challenges", Computers and Electronics in Agriculture, vol. 118, pp. 66-84, 2015 [DOI: 10.1016/j.compag.2015.08.011].

33. Rajorshee Raha, Soumyajit Dey, Pallab Dasgupta, “Adaptive Sharing of Sampling Rates among Software Based Controller”, in the proceedings of International Symposium on Intelligent Control (ISIC) under 2015 IEEE Multi-Conference on System and Control (MSC), Sydney, Australia, 21-23 September 2015.

34. Abhishek Chakraborty and Debdeep Mukhopadhyay, "A Practical Template Attack on MICKEY-128 2.0 Using PSO Generated IVs and LS-SVM", in VLSI Design (VLSID) Conference, 2016, Kolkata, India.

35. 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.

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. Sikhar Patranabis, Abhishek Chakraborty, and Debdeep Mukhopadhyay, “Fault Tolerant Infective Countermeasure for AES", in Security, Privacy, and Applied Cryptography Engineering (SPACE), 2015, Jaipur, India.

38. 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.

39. 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.

40. Amrith Krishna and Pawan Goyal, “Towards automating the generation of derivative nouns in Sanskrit by simulating Panini”, 16th World Sanskrit conference, Sanskrit and the IT world, 2015.

41. Amrith Krishna, Plaban Bhowmick, Archana Sahu, Krishnendu Ghosh, Subhayan Roy, "Automatic Generation and Insertion of Assessment Items in Online Video Courses”, in Proceedings of the 20th International Conference on Intelligent User Interfaces Companion, pp. 1-4. ACM, 2015.

42. Tanmoy Chakraborty, Amrith Krishna, Mayank Singh, Niloy Ganguly, Pawan Goyal, and Animesh Mukherjee. "FeRoSA: A Faceted Recommendation System for Scientific Articles", PA KDD, 2016.

43. Aniket Roy, Rajat Subhra Chakraborty, and Ruchira Naskar, "Reversible Color Image Watermarking in the YCoCg-R Color Space", in International Conference on Information Systems Security (ICISS), Springer International Publishing, pp. 480-498, 2015.

44. Antara Ain, António A. Bruto da Costa, Pallab Dasgupta, “Feature Indented Assertions for Analog and Mixed Signal Validation”, IEEE Transactions on CAD (Accepted).

45. Debapriya Basu Roy, Poulami Das, Debdeep Mukhopadhyay, “ECC on Your Fingertips: A Single Instruction Approach for Lightweight ECC Design in GF (p)”, in SAC-2015 (Accepted).

46. Debapriya Basu Roy, Shivam Bhasin, Sylvain Guilley, Jean-Luc Danger, Debdeep Mukhopadhyay, Xuan Thuy Ngo, Zakaria Najm, “Reconfigurable LUT: A Double Edged Sword for Security-Critical Applications”, SPACE, pp. 248-268, 2015.

47. Debapriya Basu Roy, Shivam Bhasin, Sylvain Guilley, Jean-Luc Danger, Debdeep Mukhopadhyay, “From theory to practice of private circuit: A cautionary note”, ICCD pp. 296-303, 2015.

48. Xuan Thuy Ngo, Zakaria Najm, Shivam Bhasin, Debapriya Basu Roy, Jean-Luc Danger, Sylvain Guilley, “Integrated Sensor: A Backdoor for Hardware Trojan Insertions”, DSD pp. 415-422, 2015.

49. Sikhar Patranabis, Debapriya Basu Roy, Debdeep Mukhopadhyay, “Using Tweaks To Design Fault Resistant Ciphers”, Accepted in VLSI Design, 2015 (Poster).

50. Sikhar Patranabis, Debapriya Basu Roy, Yash Shrivastava, Debdeep Mukhopadhyay and Santosh Ghosh, “Parsimonious Design Strategy for Linear Layers with High Diffusion in Block Ciphers”, in HOST, 2016 (Accepted).

51. Poulami Das, Debapriya Basu Roy, Debdeep Mukhopadhyay, “Improved Atomicity to prevent HCCA on NIST curves”, in AsiaPKC, 2016 (Accepted).

52. Debasmita Lohar, Soumyajit Dey, ”Integrating Formal Methods with Testing for Reliability Estimation of Component Based Systems”, 26th IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW), 2015.

53. M. B. Zafar, P. Bhattacharya, N. Ganguly, K. P. Gummadi, S. Ghosh, “Sampling Content from Online Social Networks: Comparing Random vs. Expert Sampling of the Twitter Stream”, ACM Transactions on the Web (TWEB), Vol. 9, No. 3, Pages 12:1--12:33, June 2015.

54. M. B. Zafar, P. Bhattacharya, N. Ganguly, S. Ghosh, and K. P. Gummadi, “On the Wisdom of Experts vs. Crowds: Discovering Trustworthy Topical News in Microblogs”, in Proc. of CSCW, San Francisco, California, USA, 2016.

55. Ranita Biswas, Partha Bhowmick, and Valentin E. Brimkov, “On the Polyhedra of Graceful Spheres and Circular Geodesics”, Discrete Applied Mathematics, 2015 (in press, DOI: http://dx.doi.org/10.1016/j.dam.2015.11.017).

56. Ranita Biswas and Partha Bhowmick, “From Prima Quadraginta Octant to Lattice Sphere through Primitive Integer Operations”, in Theoretical Computer Science, 2015 (in press, DOI: http://dx.doi.org /10.1016/j.tcs.2015.11.018).

57. Ranita Biswas and Partha Bhowmick, “On Different Topological Classes of Spherical Geodesic Paths and Circles in Z3”, in Theoretical Computer Science, Vol. 605, Pages 146-163, 2015.

58. Ranita Biswas and Partha Bhowmick, “Layer the Sphere”, The Visual Computer, Springer, Vol. 31, Pages 787-797, 2015.

59. Nabhasmita Sen, Ranita Biswas and Partha Bhowmick, “On some local topological properties of naive discrete sphere”, 6th IAPR International Workshop on Computational Topology in Image Context (CTIC), 15-17 Jun 2016, Marseille, France (to appear in LNCS proceedings).

60. Ranita Biswas and Partha Bhowmick, “On Functionality of Quadraginta Octants of Naive Sphere with Application to Circle Drawing”, 19th IAPR International Conference on Discrete Geometry for Computer Imagery (DGCI), 18-20 Apr 2016, Nantes, France (to appear in LNCS proceedings).

61. Ranita Biswas, Partha Bhowmick and Valentin E. Brimkov, “On the Connectivity and Smoothness of Discrete Spherical Circles”, 17th International Workshop on Combinatorial Image Analysis (IWCIA), 24-27 Nov 2015, Kolkata, India, LNCS 9448, pages 86-100.

62. Ranita Biswas and Partha Bhowmick, “Layer the Sphere”, TVC Special Issue Paper, 32nd Annual Conference Computer Graphics International (CGI), 24-26 June 2015, Strasbourg, France.

63. Dhruv Jain, Swapnil Agarwal, Satadal Sengupta, Pradipta De, Bivas Mitra, Sandip Chakraborty, “Prediction of Quality Degradation for Mobile Video Streaming Apps: A Case Study using YouTube”, in Poster Track of the 8th International Conference on Communication Systems and Networks (COMSNETS), Bangalore, India, January 2016 [Best Poster Award].

64. Satadal Sengupta, Harshit Gupta, Pradipta De, Bivas Mitra, Sandip Chakraborty, Niloy Ganguly, “Understanding Data Traffic Behaviour for Smartphone Video and Audio Apps”, in Poster Track of the 8th International Conference on Communication Systems and Networks (COMSNETS), Bangalore, India, January 2016.

65. Chander Govindarajan, Satadal Sengupta, Pradipta De, Bivas Mitra, Sandip Chakraborty, “Role of Network Control Packets in Smartphone Energy Drainage”, in Poster Track of the 8th International Conference on Communication Systems and Networks (COMSNETS), Bangalore, India, January 2016.

66. Urbi Chatterjee, Rajat Subhra Chakraborty, Hitesh Kapoor, Debdeep Mukhopadhyay. “Theory and Application of Delay Constraints in Arbiter PUF", accepted in ACM Transaction on Embedded Computing Systems.

67. Urbi Chatterjee, Rajat Subhra Chakraborty, Jimson Mathew, Dhiraj K. Pradhan. “Memristor based Arbiter PUF: Cryptanalysis Threat and its Mitigation", in International Conference on VLSI Design (VLSID), 2016.

68. Barsha Mitra, Shamik Sural, Vijayalakshmi Atluri, and Jaideep Vaidya, “The generalized temporal role mining problem”, Journal of Computer Security (JCS) (SCOPUS Indexed), Vol. 23(1), pages 31-58, March 2015.

69. Barsha Mitra, Shamik Sural, Jaideep Vaidya, and Vijayalakshmi Atluri, “A Survey of Role Mining”, ACM Computing Surveys, Vol. 48(4), 2016 (DOI: 10.1145/2871148).

70. Shrutilipi Bhattacharjee and Soumya K. Ghosh, “Spatio-temporal Change Modeling of LULC: A Semantic Kriging Approach”, ISPRS Annals of the Photogrammetry, Remote Sensing and Spatial Information Sciences, vol. II-4, no. W2, pp. 177-184, July 2015.

71. Shrutilipi Bhattacharjee and Soumya K. Ghosh, “Performance Evaluation of Semantic Kriging: A Euclidean Vector Analysis Approach”, IEEE Geoscience and Remote Sensing Letters, vol. 12, no. 6, pp. 1185-1189, June 2015.

72. Shrutilipi Bhattacharjee, “Prediction of Meteorological Parameters: A Semantic Kriging Approach”, 23rd ACM SIGSPATIAL International Conference on Advances in Geographic Information Systems (ACM SIGSPATIAL 2015) PhD Symposium, Seattle, Washington, USA, November 3, 2015.

73. Shrutilipi Bhattacharjee and Soumya K. Ghosh, “Time-Series Augmentation of Semantic Kriging for the Prediction of Meteorological parameters”, 28th IEEE International Geoscience and Remote Sensing Symposium (IGARSS 2015), pp. 4562-4565, Milan, Italy, July 26-31, 2015.

74. S. Misra, S. Goswami, C. Taneja, A. Mukherjee, and M. S. Obaidat, “A PKI adapted model for secure information dissemination in industrial control and automation 6LoWPANs”, in IEEE Access Journal, vol. 3, pp. 875-889, 2015.

75. S. Misra and S. Goswami, “Cognitive prediction of end-to-end bandwidth utilization in a non-QoS video conference”, in IEEE ICC, pp. 6152-6156, June 2015.

76. S. Sarkar, S. Chatterjee, and S. Misra, “Analysis of Fog Computing: The Convergence of Cloud Computing to Green Computing", in IEEE Transactions on Cloud Computing, 2015.

77. S. Chatterjee, S. Misra, and S. U. Khan, “Optimal Data Center Scheduling for Quality of Service Management in Sensor-cloud", in IEEE Transactions on Cloud Computing, 2015.

78. S. Chatterjee, R. Ladia, and S. Misra, “A Dynamic Optimal Pricing Scheme for Heterogeneous Service-Oriented Architecture for Sensor-cloud Infrastructure", in IEEE Transactions on Services Computing, 2015.

79. S. Misra, A. Singh, S. Chatterjee, and A. K. Mandal, “QoS-Aware Sensor Allocation for Target Tracking in Sensor-Cloud", in Ad Hoc Networks, Elsevier, 2015.

80. S. Sarkar, S. Chatterjee, and S. Misra, “Evacuation and Emergency Management Using a Federated Cloud", in IEEE Cloud Computing Magazine, 2015.

81. S. Chatterjee, and S. Misra, “QoS Estimation and Selection of CSP in Oligopoly Environment for Internet of Things", in IEEE WCNC, 2016.

82. S. Chatterjee, and S. Misra, “Optimal Composition of a Virtual Sensor for Efficient Virtualization Within Sensor-cloud", in IEEE ICC, 2015.

83. S. Chatterjee, and S. Misra, “Quantification of Node Misbehavior in Wireless Sensor Networks: A Social Choice-Based Approach", in IEEE ICC Workshop, 2015.

84. S. Chatterjee, S. Sarkar, and S. Misra, “Energy-Efficient Data Transmission in Sensor-Cloud", in International Conference on Applications and Innovations in Mobile Computing (AIMoC), 2015.

85. P. V. S. R. Teja, S. Chatterjee, S. N. Das, and S. Misra, “Two-Level Mapping to Mitigate Congestion in Machine to Machine (M2M) Cloud", in International Conference on Applications and Innovations in Mobile Computing (AIMoC), 2015.

86. Debapriya Basu Roy, Poulami Das, Debdeep Mukhopadhyay, “ECC on Your Fingertips: A Single Instruction Approach for Lightweight ECC Design in GF (p)”, in SAC, 22nd International Conference on Selected Areas in Cryptography, 2015.

87. Poulami Das, Debapriya Basu Roy, Debdeep Mukhopadhyay, “Exploiting the Order of Multiplier Operands: a Low-cost Approach for HCCA Resistance”, in IACR Cryptology ePrint Archive 2015.

88. Poulami Das, Debapriya Basu Roy, Debdeep Mukhopadhyay, “Improved Atomicity to prevent HCCA on NIST curves”, in ASIAPKC, 3rd ACM ASIA Public-Key Cryptography Workshop, 2016.

89. Christina Boura, Avik Chakraborti, Gaetan Leurent, Goutam Paul, Dhiman Saha, Hadi Soleimany, Valentin Suder, “Key Recovery Attack against 2.5-round π-Cipher”, to appear In Proceedings of 23rd International Conference on Fast Software Encryption, FSE 2016.

90. Dhiman Saha, Dipanwita Roy Chowdhury, “SCOPE: On the Side-channel Vulnerability of Releasing Unverified Plaintexts”, in Proceedings of the 22nd Conference on Selected Areas in Cryptography, SAC 2015.

91. Shamit Ghosh, Dhiman Saha, Abhrajit Sengupta, Dipanwita Roy Chowdhury, “Preventing Fault Attack Using Fault Randomization With a Case-Study on AES”, in Proceedings of the 20th Australasian Conference on Information Security and Privacy, ACISP 2015.

92. Dhiman Saha, Dipanwita Roy Chowdhury, “Diagonal Fault Analysis of Groestl in Dedicated MAC Mode” , In Proceedings of IEEE Int. Symposium on Hardware-Oriented Security and Trust, HOST 2015.

93. Rohit Verma, Aviral Shrivastava, Bivas Mitra, Sujoy Saha, Niloy Ganguly, Subrata Nandi, and Sandip Chakraborty. “UrbanEye: An Outdoor Localization System for Public Transport”, in IEEE INFOCOM 2016.

# Research Scholars Who Graduated in 2015 – 2016

## PhD Students

1. **Bibhas Ghoshal**
2. **Sudipta Saha**
3. **Sanjay Chaterji**
4. **Bodhisatwa Mazumdar**
5. **Sabyasachi Karati**
6. **Tapas Samanta**
7. **Aritra Hazra**
8. **Sourav Kumar Dandapat**
9. **Tripti Swarnkar**
10. **Sanjoy Pratihar**
11. **Tanmoy Chakraborty**
12. **Joy Chandra Mukherjee**
13. **Kamalesh Ghosh**
14. **Sumanta Pyne**
15. **Kunal Banerjee**

## MS Students

1. **Swadhin Pradhan**
2. **Souvik Kolay**
3. **Pranab Kumar Chanda**
4. **Partha De**
5. **Debapriya Basu Roy**
6. **Abhrajit Sengupta**
7. **Shamit Ghosh**