
# research scholars' day 2014

IIT Kharagpur

# 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 fifth Research Scholar Day is going to be celebrated on the 9th day of March, 2014. This event gives the research students and the faculty members a unique opportunity to share and exchange research ideas and to build a complete picture of the research activity carried out by the research scholars in the department. The day also provides the research scholars with a platform to publicly demonstrate their cultural aptitude. Like the previous years, this year too the day will be observed with enthusiasm and zeal by our PhD and MS students. Let me wish this event a grand success!***

***Rajib Mall***
***Head of the Department***

*The charcoal sketch of the Department on the front cover was created by Romil Roy. The photo of the CSE Annex Building on Page 1 was taken on the Research Scholar Day of 2013. The sketch of the main building on the back cover was taken from the Institute's website. The cover-design team includes Shashaank M. Aswatha, M. Srinivas Virinchi, and Dhiman Saha. The production team for this brochure consists of Aritra Hazra, Dhiman Saha, Sabyasachi Karati, Sandipan Sikdar, Suvadeep Hajra, and Tanmoy Chakraborty. Other volunteers include Ashok Das, Ayan Palchaudhuri, Bappa Chowdhury, Bivas Ghosal, Rajesh, Ranita Biswas, Somyadip Bandyopadhyay, and Sourya Bhattacharyya. Help and cooperation from all research scholars, faculty members, and staff members of the CSE Department are highly appreciated.*

## List of Current PhD Scholars

**Abir De**
**Anju P J**
**Anupam Mandal**
**Aritra Hazra**
**Ayan Das**
**Bibhas Ghoshal**
**Bijju Kranthi Veduruparthi**
**Bodhisatwa Mazumdar**
**Debashis Mukherjee**
**Dhiman Saha**
**Durga Prasad Sahoo**
**Jimmy Jose**
**Joy Chandra Mukherjee**
**Kajori Banerjee**
**Kamalesh Ghosh**
**Koustav Rudra**
**Kunal Banerjee**
**Manjira Sinha**
**Mayank Singh**
**Moumita Saha**
**Papia Mahato**
**Parantapa Bhattacharya**
**Priyanka Sinha**
**Rajendra Prasath R**
**Rajib Lochan Jana**
**Rajorshee Raha**
**Ranita Biswas**
**Rishiraj Saha Roy**
**Sabyasachi Karati**
**Sandip Karmakar**
**Sandipan Sikdar**
**Sanjoy Pratihar**
**Sarani Bhattacharya**
**Saurav Kumar Ghosh**
**Shyantani Maiti**
**Soma Saha**
**Soumajit Pramanik**
**Soumyadip Bandyopadhyay**
**Sourav Kumar Dandapat**
**Sourya Bhattacharyya**
**Subhasish Dhal**
**Subhrangsu Mandal**
**Sudakshina Datta**
**Sudipta Saha**
**Suman Kalyan Maity**
**Sumana Ghosh**
**Sumanta Pyne**
**Tanmoy Chakraborty**
**Tanwi Mallick**
**Tapas Kumar Mishra**
**Tirthankar Dasgupta**
**Tripti Swarnkar**

## List of Current MS Scholars

**Abhishek Chakraborty**
**Abhrajit Sengupta**
**Anirban Ghose**
**Arnab Dhar**
**Ayan Palchaudhuri**
**Debapriya Basu Roy**
**Debasmita Lohar**
**Parnab Kumar Chanda**
**Partha De**
**Sayandeep Saha**
**Shamit Ghosh**
**Shiladitya Ghosh**
**Souvik Kolay**
**Srinivas Virinchi**
**Suvadeep Hajra**
**Swadhin Pradhan**

# PhD Scholars


**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

**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, is 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.

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

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

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

## Formal Methods for Architectural Power Intent Verification and Functional Reliability Analysis

The growing complexity of modern-day system designs aspires newer development and engineering challenges. The current trend towards handling large industrial designs is to build the overall system in a top-down hierarchical manner, starting from the architectural requirements and gradually forming the component-level plans. During the development phase of such component-based hierarchical systems, the designers need to guarantee four critical aspects of design, namely – *functional correctness*, *end-to-end timing*, *power performance* and *functional reliability*. A significant amount of research has been conducted on the functional (behavioral) aspects of such complex designs, namely, correctness and timing. The correctness and completeness of large systems are ensured via design intent verification and model checking paradigms. Recently, timing/performance analysis of component-based designs are also looked upon, which enables proper end-to-end functional behaviors of complex hierarchical systems.

However, there has been a lack of effort in formalizing and analyzing the two important non-functional (performance) aspects, namely *architectural power intent* and *functional reliability*, at an early-stage of component-based hierarchical systems. With a rapid increase in the complexity of designs, meeting a stringent low-power budget by efficient global power management schemes becomes an important issue now-a-days. This gives rise to the necessity of an early-stage verification framework for the architectural power intent of designs. Since the power management logic as well as the power performance varies with the selection of power domain partitions, hence there is also a need to determine the power usage at an early-stage of the design flow and converge into the best power domain partitions before the power management logic is laid out.

Recent research has indicated ways of using unified power format (UPF) specifications for extracting valid low-level control sequences to express the transitions between the power states of individual domains. Today there is a disconnection between the high-level architectural power management strategy which relates multiple power domains and these low-level assertions for

controlling individual power domains. Our work presents a verification framework that attempts to bridge the disconnect between high-level properties capturing the architectural power management strategy and the implementation of the power management control logic using low-level per-domain control signals. The novelty of the proposed framework is in demonstrating that the architectural power intent properties developed using high-level artifacts can be automatically translated into properties over low-level control sequences gleaned from UPF specifications of power domains, and that the resulting properties can be used to formally verify the global on-chip power management logic. The proposed translation uses a considerable amount of domain knowledge and is also not purely syntactic, because it requires formal extraction of timing information for the low-level control sequences. In addition to this, the completeness of the global power management logic also needs to be examined formally by the help of its global power state coverage. The architectural power intent of a design defines the intended global power states of a power-managed integrated circuit. Verification of the implementation of power management logic involves the task of checking whether only the intended power states are reached. In this work, we present a formal method for determining the set of reachable global power states in a power-managed design. Our approach demonstrates how this task can be further constrained as required by the verification engineer. In our work, we also developed a tool, called *POWER-TRUCTOR* which enables the proposed framework to guarantee the correctness and completeness of a global power manager.

Moreover, formal certification of correctness has been included in the safety standards for several domains, including aeronautics, automotive, industrial process automation), nuclear, railway and space. We believe that formalizing the notion of reliability and overlaying reliability specifications on the functionality of a design will become an important requirement in the future. Typically, the necessity to attain higher reliability in safety-critical component-based systems is overcome by introducing various fault-tolerance methods leveraging spatial and temporal redundancy in these systems. Therefore, the reliability preserving system specifications need to incorporate such spatial and temporal redundancies in order to dictate a more reliable implementation of the system. The process of incorporating appropriate component-level reliability prescriptions introduces a newer challenge of computing the reliability for component as well as system properties at an early-stage. Typically, the computation of the reliability of an integrated system is carried out from the given reliability measures of its components, where the notion of component failure is defined with respect to the component as a whole. However, our focus is on specific safety-critical functionalities of the component that affect a given set of end-to-end feature requirements. In our work, we study the problem of assessing *feature/specification reliability*, that is the reliability of an end-to-end property of the system. We present a formulation of the reliability gap for given reliability values of the different component-level formal properties and formally characterize the solution space to meet this gap. Given the range of reliability choices for each component property, we also propose a divide-and-conquer algorithm to bridge the reliability gap.

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

***Supervisor: Prof. Sourangshu Bhattacharya***

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

## Distributed Regularized Loss Minimization

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

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

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

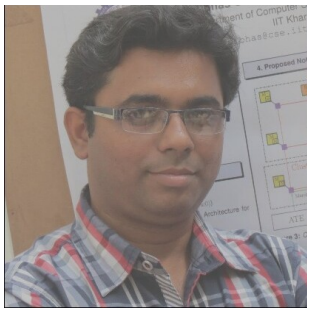
We use a master-slave architecture to solve this problem where all the sites containing the training data (slave) are connected to the central computer(master). Given this distributed setting, alternating direction method of multipliers provides a framework for implementation of the loss minimization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

**References**


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

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

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



**Bibhas Ghoshal**
Email: bibhas@cse.iitkgp.ernet.in
Joined the department in: December 2009

***Bibhas Ghoshal*** *is pursuing PhD in Computer Science and Engineering from IIT Kharagpur. His recent research activities have been in the areas of VLSI testing. He holds ME (2005) in Computer Science and Engineering from West Bengal University of Technology and M.Sc (2002) degrees in Electronic Science from Jadavpur University.*

***Supervisor: Prof. Indranil Sengupta***

## Devising Improved Techniques for Testing Embedded Memory Sub-systems in Systems-on-Chip

Designers using bus based interconnect network for System-on-Chip (SoC) designs often face difficulty related to bandwidth, signal integrity, and power dissipation of the chip. The Network-on-Chip (NoC) communication architecture has emerged as an acceptable solution to solve these issues. In a NoC-based chip, the communication network consists of network interfaces (NI), routers, and channels to connect the routers. The cores communicate among each other by sending and receiving packets. However, like all other SoCs, NoC based SoCs must also be tested for manufacturing defects. Majority of work reported in literature focus on finding improved test techniques for logic cores interconnected using NoC. However, embedded memory content in NoC based systems have increased from one-tenth to more than three fourth of the chip area today and will continue to increase. Due to their high density, these embedded memories are more prone to manufacturing defects than other type of on-chip circuits.

To the best of our knowledge, not much research has been done on exploring test techniques for the NoC based memory cores. One probable reason may be acceptance of Built-In-Self-Test (BIST) as the most preferred technique for testing memories. Employing Memory BIST (MBIST) does not need any test access mechanism (TAM), as tests generation as well as comparison of results are done locally. However, MBIST for memories connected using NoC also face the same test challenges as faced by any other BIST technique for embedded memories. Unless carefully designed, NoC based MBIST may induce excessive power, in addition to performance and area overhead. Thus, there is a need for research in finding efficient test techniques for memory cores which are interconnected using NoC at minimum area overhead and optimized test time and test power. Moreover, it must be also be ensured that the elements of NoC are fault free so that the NoC can be re-used for test of the interconnected cores.

The objective of the research has been to devise cost effective test techniques for memory modules in a NoC based memory system, targeting minimum area overhead at optimized test time and test power. The research was aimed at improving the existing approaches of test of NoC based memory cores along the following directions.

1. Test Architecture: In case of SRAMs, a distributed architecture was proposed to allow hardware sharing and eventually reduction of area overhead due to test circuitry. Moreover, the proposed architecture tried to incorporate the advantages of both parallel and serial testing

approaches to optimize test time. For DRAMs, we tried to re-use the on-chip resources such as refresh circuit for test purpose. Re-using refresh for test avoided use of extra DFT logic, bringing down area overhead. It also saved read cycles during March test operation on the DRAM, as read operations were performed during refresh. Moreover, test circuit for each type of memory was designed for programmability, to support multiple test algorithms for higher fault coverage. The test techniques were initially developed for single memory module and then were extended for test of number of modules.

2. Test scheduling algorithms - For optimized time and power during test of number of memory cores, improved test architectures should be supplemented by efficient test scheduling algorithms. For each of the test architectures proposed in the research, a test scheduling algorithm was proposed focussing on improvements in two directions. First, to limit the number of concurrent test blocks under power constraints and second, to reduce the switching activity during test.

3. Modified test algorithms for on-line test - Recent studies of memory failures in field gave strong evidence that memories when deployed for field operation experience permanent faults more than transient faults. The soft error data detection schemes are not sufficient for testing in field permanent faults as these schemes do not perform active test – they do not alter the contents of the memory. Therefore, the research was aimed at finding a cost effective on-line test technique that can detect permanent faults during field operation of memories. To perform an active test, March based tests are mostly preferred due to their high fault coverage. However, performing March test on a memory involves writing predefined test patterns into memories and reading the same. Such a technique is allowed during manufacturing test but cannot be afforded for in-field operation where the normal operation resumes after test. Thus, we preferred transparent March tests in place of standard March tests. Transparent testing is a technique where the original contents of the memory remain unchanged after test. Two on-line transparent test techniques have been proposed. The first transparent test technique was targeted for permanent faults developed during field operation of DRAMs. The test was performed during refresh cycles of the DRAM. Reusing refresh allowed periodic testing of DRAM without interruption while overcoming the requirement of additional Design-For-Testability (DFT) hardware. The second proposed transparent test technique was targeted for detection of permanent faults developed in FIFO buffers during field operation of NoC.

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

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

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

## Lung Tumor Identification and Modeling for Radiation Treatment Planning

Lung cancer is one of the most common cancer in the world with the highest morbidity and mortality. Identifying tumor lesions at an earlier stage will help us direct treatment of the patient using radiation/surgery before the tumor becomes cancer.

### Tumor Identification

On several occasions it takes an expert to exactly pinpoint the location of tumor and delineate the tumor from the non-cancerous tissues. Therefore computing methods have to be introduced which can assist doctors and radiologists in the identification of cancer. An identified cancer poses several challenges to estimate the radiation therapy course to be taken for the treatment of the patient. Imaging techniques for the classification and delineation of primary lung tumors and lymph nodes are a prerequisite for adequate radiotherapy. Prediction of the outcome of radiation therapy can further help doctors in making decisions if radiation therapy or surgery is more suitable.
Our current research focuses on tumor delineation using the gradient in PET images for tumor measurement and CT images for identification of initial tumor location.

### Cancer modeling

Another ongoing research concerns about construction of 3D model of the cancer in the lung using the stack of 2D images of PET and CT. Computational modeling of the stages of lung cancer can help doctors identify the current stage of a potential cancer patient and predict the treatment to be taken. The computational model helps in simulating the cancer development and spread in the lung which can help doctors pinpoint the cancer location for either radiotherapy or surgery.

**Bodhisatwa Mazumdar**
Email: bodhisatwa@cse.iitkgp.ernet.in
Joined the department in: July 2009

***Bodhisatwa Mazumdar*** *received a B.Tech. degree in Electronics and Instrumentation Engg. from University of Kalyani, Kalyani in 2004, and an M.S. degree in Electronics and Electrical Communication Engg from Indian Institute Institute of Technology, Kharagpur in 2007. From September 2007 till May 2008, he worked in GE Healthcare, Bangalore, as a Hardware Design Engineer. Since May 2008 to July 2009 he worked as Member Technical Staff in Manthan Semiconductors Pvt. Ltd., Bangalore. Since July 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 Cryptography and Network Security.*

***Supervisors: Prof. Debdeep Mukhopadhyay and Prof. Indranil Sengupta***

## Design for Security of Block Cipher S-Boxes to Resist DPA Attacks

As communication networks are spreading by leaps and bounds, the need for secured communication and hence fast but secured cryptographic systems is growing bigger. This necessitates the call for "Design for Security" which entails design, implementation and security of cryptographic hardware and embedded systems. Block cipher cryptosystems embedded in cryptographic devices are susceptible to attacks which show that security cannot be an afterthought. Like as performance, testability are important issues which the designer takes care in the design cycle, security also has to be taken into consideration early in the design cycle. As a motivating example, differential power analysis (DPA) attacks and vulnerability modeling of cryptographic devices have shaken the strength of cryptographic implementations and have baffled the designers for the past fifteen years that a very strong mathematical algorithm can be compromised using these powerful techniques. The Advanced Encryption Standard (AES) was found to be compromised, despite being a mathematically strong cipher. Literature shows that S-boxes, the nonlinear components in the cipher are responsible for its vulnerability towards DPA.

The asymmetry in the power consumption of transitions of bit values from 0 to 1, and 1 to 0 in the CMOS library are the root cause for such attacks. Countermeasures like gate-level masking and several algorithmic countermeasures have been discovered but they were found to be costly in terms of hardware footprint and power consumption. Also some of these countermeasures are prone to higher-order differential side channel attacks. Most importantly, they make AES like block cipher algorithms so poor in performance that they rob the algorithm from its mathematical elegance and efficient performance, some of the prime reasons why Rijndael algorithm emerged as the AES.

With this motivation, the current research work investigates whether Boolean functions involved in the AES S-Box can be designed with security as an objective from the beginning. In the first step, we have proposed a RAIN S-Box whose construction and design makes it more DPA resistant than the AES Rijndael S-Box while having similar classical cryptographic properties like SAC, nonlinearity, balancedness, propagation characteristics (PC) and correlation immunity (CI). Also the parameter, transparency order which quantifies DPA resistance of the S-Box is found to be smaller than the Rijndael inverse S-Box and has been practically shown to require more number of power

traces to attack the cipher. This confirms that the nature of Boolean functions have strong role not only on the mathematical robustness but also on the resistance to attacks which exploit side-channel information leakage like power. At present, we attempt to synthesize a class of balanced Boolean functions which have both above-mentioned important cryptographic properties and higher resistance DPA attacks defined in terms of parameters like transparency order and SNR (DPA). This involves proposing heuristic searching algorithms to find DPA resistive Boolean functions in the class of Rotation Symmetric Boolean Functions (RSBFs) which work towards optimizing a cost function in terms of Walsh spectra and autocorrelation functions of the coordinate functions of an S-Box. Also a construction algorithm for Rotation Symmetric S-Boxes (RSSBs) using these high nonlinearity RSBFs is proposed. The S-Boxes on practical evaluation of DPA attacks show requirement of much higher number of power traces to reveal the secret key when compared to the standard AES Rijndael S-Box.

**Debashis Mukherjee**
Email: debashis_mukherjee@yahoo.com
Joined the department in: January 2014

***Debashis Mukherjee*** *joined the Department of Computer Science and Engineering recently. He will carry out his research work in the area of software engineering.*

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

**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: December 2011

***Durga Prasad Sahoo*** *received B.Sc. degree in Computer Science from Ramakrishna Mission Residential College, University of Calcutta, Kolkata in 2007; M.Sc. degree in Computer and Information Science from University of Calcutta, Kolkata in 2009 and M.Tech. degree in Computer Science from University of Calcutta, Kolkata in 2011. From August 2011 till December 2011, 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 Algorithm design, Graph Theory and Hardware Security.*

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

## Machine Learning based Model-building Attacks on 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.

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

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

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

## Design and Analysis of Scalable Parameterized Stream Ciphers

Stream Cipher is an important branch in symmetric key cryptography. The goal of a stream cipher design is that it must provide high-speed encryption and less design overhead in comparison with block ciphers. A number of stream ciphers are reported in eStream project among which some are hardware efficient whereas some are software efficient. On the other hand, stream ciphers with the goal of receiving higher throughput than the eStream ciphers are also reported in literature. However, design of scalable parameterized stream ciphers with flexible design option to optimize speed vs area is a recent challenge. This PhD work aims to study the standard eStream ciphers and to propose compact design with high throughput and less area. This research also includes the cryptanalysis of these new stream ciphers.

One of the methods of cryptanalysis on stream ciphers is the fault attack. These types of attacks were later improved by algebraic techniques. Trivium, one of the finalists in eStream project, is also susceptible to fault attack. The attack exploits the fact that the non-linearisation process of Trivium is very slow. Our work is now focused on how fault attacks can be prevented in Trivium like ciphers.

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

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

***Supervisor: Prof. Arobinda Gupta***

## Scheduling in Large Scale Mobile Networks

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

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

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

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

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

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

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

**Kajori Banerjee**
Email: kajori.bn@gmail.com
Joined the department in: July 2013

***Kajori Banerjee*** *completed her B.Tech. degree in Computer Science & Engineering Department from Netaji Subhash Engineering in 2011. She first joined this department in as a M.Tech student and received her degree in 2013. Currently, she has been working as a Ph.D. student. Her research interests are in the areas of Formal Verification, Real Time, Hybrid and Embedded Systems , Logic and Automata theory.*

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

## Event Sequences under Real Time Calculus Constraints

In recent times, Real Time Calculus (RTC) has been extensively used to provide a succinct summary for event patterns in complex networked embedded systems. A RTC constraint specifies a lower and upper bound on the number of events in a given interval of time. The goal was developing an automata theoretic approach for generating random event sequences satisfying a specification in Real Time Calculus. This problem is non-trivial because not all valid finite event patterns could be extended to a valid infinite event sequence. Therefore, a less informed generator could reach a forbidden state from which it was impossible to proceed without violating a constraint. We showed that the patterns, satisfying a given finite set of RTC constraints, defined an interesting fragment of ω - regular languages and demonstrated an approach for developing a generator for sequences defined by the RTC constraints.

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

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

***Supervisor: Prof. Pallab Dasgupta***

## Formal Methods for Top-Down Component Based

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

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

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

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

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

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

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

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

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

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

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

Online social networks (OSNs) like Twitter 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.

**Kunal Banerjee**
Email: kunal.banbros@gmail.com
Joined the department in: January 2010

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

***Supervisors: Prof. Chittaranjan Mandal and Prof. Dipankar Sarkar***

## Validation of Transformations of Embedded System Specifications Using Equivalence Checking

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

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

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

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

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

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

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

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

***Supervisor: Prof. Anupam Basu***

## Text Readability and Enhancement

Often, after going through a piece of text, the first criteria by which we judge is the 'readability' of the text. Though we cannot always concretely parameterize, generally it refers to the fact that how well we have grasp the content. 'Readability' is the ease with which a text can be read and understood. It plays a significant role in the design of texts which match to the target populations' skill. Readability has been measured using a number of factors from both the reader's and the text sides. Readability depends on the reader's physical and cognitive abilities as well as social and economic background. For text, readability is generally defined by four top level features: coherence, style, format and organization. Apart from the reader and the text, readability also gets affected by the communicating language. Every language has some unique properties and any effective metric of readability has to take these into account.

English has a long history of readability research starting from 1880. From then, it has come a long way from early subjective evaluation techniques to statistical measures and empirical formulas, from addressing the child population to investigate the reading choices and availabilities for adults. In the beginning, metrics were based on 'vocabulary frequency list', then afterwards, formulas like Flesch index, Fog index etc. incorporated the structural features of a text, and now a days we have measures which takes into account the higher level cognitive features like text cohesion and coherence, e.g. coh-metrix.

In case of Indian languages, especially Bangla, such extensive research work is still unavailable. There are applications of the known readability formulas of English to measure the readability of Bangla texts. The problem in this approach is that Bangla as a language has some distinguishing properties than English, therefore, the formulas applicable to English do not yield the correct results when implanted unchanged in Bangla. Another important aspect of readability, as mentioned above is to customize texts for different reader groups. In the context of a country like India, this is the need of the hour in every level of formal or informal education. If we consider the case of textbooks at the school level, we will see that a majority of both the students and teachers find them extremely hard to comprehend and retain. In addition to this, for a language like Bangla, geographical variations of the language-usage come into play.

To address these and to provide an effective framework for designing textbook contents in Bangla, measures have to be taken at different levels of hierarchy taking into account the backgrounds of both teachers and students; the levels are defined as:

1. The bottom layer will deal with the lexical choices, that is, which word to use to describe a concept.

2. This layer will analyze the relative difficulties of the different sentence structures.

3. The purpose of this layer will be to study the organization of the discourse and measures of its local and global coherence.

4. At the top level, the balance between diagrams and texts will be considered.

As can be seen the bottom two levels will take into account the language specific features and the top two levels will deal with the cognitive and psycholinguistics sides. In this way, it will be possible to have a complete approach towards enhancing the acceptability of textbooks.

**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.

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

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

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

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

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

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

## Topical Search in Twitter Online Social Network

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

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

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

**References**


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

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

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

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

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

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

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

***Priyanka Sinha*** *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. She was awarded the Institute Merit Award from 2000-2002 and was a Vodafone fellow from 2005-2006. She has been a Graduate Teaching Assistant, a Graduate Research Assistant and a Graduate Fellow. She is a scientist at Innovation Lab, Tata Consultancy Services Limited, Kolkata. She has worked on the SmartEdge 800 at Redback Networks, An Ericsson Company, and on interactive TV at ITAAS India Private Limited. Her research interests are in the broad area of computer systems, networking, security, wireless, text mining and ubiquity. She is currently pursuing PhD in Computer Science and Engineering from IIT Kharagpur.*

***Supervisors: Prof. Pabitra Mitra and Prof. Anupam Basu***

## Text Mining

Currently I plan to work on mining text from social media for use cases in healthcare, in particular elderly people care, for example, using text analytics finding trends in people's conversation online to identify whether they suffer from any mental disorders, etc. Parallel to this work is to find out if people conversing in a company-wide social media are suffering from any technical challenge and redirect them to possible solutions.

**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.*

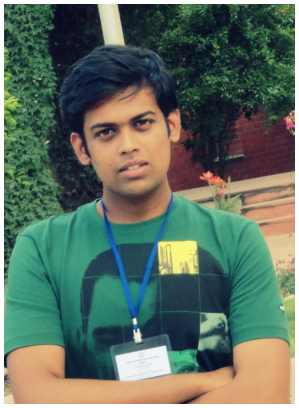
***Supervisor: Prof. Sudeshna Sarkar***

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

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

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

Rajib Lochan Jana joined the Department of Computer Science and Engineering recently. He will carry out research in the area of formal methods for embedded system design.



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

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

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

## Validation of Embedded Real Time Control

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

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

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

**References**


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

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

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

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

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

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

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

***Ranita Biswas*** *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, Computer Graphics, Image Processing and Pattern Recognition.*

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

## Digital Spheres and Geodesics: Characterizations, Algorithms, Applications

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

We have so far worked on topologically well-defined models of 3D digital spheres using graph-theoretic and number-theoretic techniques. We have designed an algorithm to generate a 3D digital sphere having integer radius and integer center. The algorithm evolves from novel number-theoretic characterization, and is marked by purely integer operations, easy implementation, efficiency, and exactness. We have currently designed an algorithm for finding *discrete geodesic paths* on the surface of a digital sphere, supplied the source and the destination points. This algorithm is output-sensitive and runs in optimal time, as it is designed out of the number-theoretic properties of digital sphere.

Our further research work includes identification of *persistent patterns* in a digital sphere and generation of *iso-contours* on digitized 3D surfaces.

**Rishiraj Saha Roy**
Email: 10cs9401@iitkgp.ac.in , rishiraj.saharoy@gmail.com
Joined the department in: January 2010

***Rishiraj Saha Roy*** *received a B.E. degree in Information Technology from Jadavpur University, Kolkata in 2007, and an M.Tech. degree in Information Technology from Indian Institute of Technology Roorkee in 2009. Since December 2009, he has been a research scholar in the department of Computer Science and Engineering at IIT Kharagpur. His research interests are in the areas of Information Retrieval and Complex Networks. He was awarded the Microsoft Research India Ph.D. Fellowship in 2011.*

***Supervisor: Prof. Niloy Ganguly and Dr. Monojit Choudhury (Microsoft Research India)***

## Analyzing Linguistic Structure of Web Search Queries

Current search engines consider a query to be a bag-of-words and assume that a relevant document will have all or most of the keywords; stop words such as in, of, and why, are ignored altogether. Motivation for this work stems from the fact that there is much more inside a query than just its constituent terms. For example, the query "can't view large text files in windows 7" is definitely not the same as an unordered list of its constituent terms – can't, view, large, text, files, windows and 7. More often than not search engines return very unsatisfactory results for this type of queries, because they ignore the facts that here large text files is an entity, can't view is an action on large text files, and in indicates that the rest of the query is in the context of the windows 7 operating system. Ironically, this seems to happen when the user tries to specify the information need a bit more precisely.

The aim of the proposed research is to understand the underlying structure of queries, learn those structural units and patterns automatically from data and apply this knowledge to improve the performance of search engines. We can intuitively feel that English language grammar, which is so essential to the understanding of natural language phrases and sentences, does not hold for Web queries. If we compare a Web search query and its corresponding natural language sentence or phrase, we would often observe that many words have been dropped while forming the query. Also, there is more flexibility in the relative ordering of the words in the query – two queries can be semantically equivalent even if the ordering of the words varies to a large extent. These issues propel us to formulate a new grammar for queries – which we can extract from the data, based upon our structural organization. Once we have a working definition of a grammar in place, the next task would be parsing a query in accordance with this grammar. We foresee that if we are able to grasp the internals of a query at this level, we can use this knowledge to bring about great improvements in search quality by enhancing established techniques like query expansion and re-ranking the list of search results.

To this end, we plan to apply machine learning techniques on data resources such as query logs, click-through data, per user sessions' data, and the contents of Web documents. This would require rigorous manual analysis of query logs to understand the structural patterns of queries. Past work has talked about intent of a query as a whole [1, 2]. But our initial study shows us that the words in a query itself can be grouped into two classes, which we shall call content and intent words (or phrases). While content words are like keywords that must be matched at the document side, intent words can be used to guide the search engine in other ways. We note that labelling as content or intent is not at the word level but for meaningful expressions as a whole. This motivates us to devise a

suitable scheme to perform query segmentation (breaking a query into its meaningful segments). After observing and annotating a large amount of query logs, we came up with a robust linguistic classification of intent words. These rules were derived from first principles and based on the nature of interaction between content and intent words. We found that well-established statistical techniques can be used to perform query segmentation (with the segments thus obtained aligning satisfactorily with our notions of content and intent) as well as distinguish between content and intent words. Our results also have a good degree of concordance with data annotated by humans.

We propose to make significant progress in the foregoing lines of thought. We believe that the overall idea is capable of introducing a new paradigm in Web search – trying to understand the meaning of a user query from its structure before actually diving in to retrieve the results. We also foresee that as we go along, we would also be able to shed light on various other interesting phenomena – the learning curve of users when it comes to being successful in Web search, search patterns of users from different geographical locations, and customizing results based on search patterns of individual users.

**References**

[1] A. Broder, "A Taxonomy of Web Search", ACM (Association for Computing Machinery) SIGIR (Special Interest Group on Information Retrieval) Forum, Volume 36, Issue 2 (Fall 2002), 2002, ACM, New York, USA, pages 3–10.

[2] J. Jansen, D. L. Booth, and A. Spink, "Determining the informational, navigational, and transactional intent of Web queries", in Information Processing and Management (IPM), Volume 44, Number 3, May 2008, Pergamon Press, Inc., New York, USA, pages 1251–1266.

**Sabyasachi Karati**
Email: skarati@cse.iitkgp.ernet.in, sabyasachi.karati@gmail.com
Joined the department in: July 2010

***Sabyasachi Karati*** *received his B.E. degree in Computer Science & Engineering from Jadavpur University, Kolkata in 2008 and M.Tech.degree in Computer Science & Engineering from IIT Kharagpur, Kharagpur, West Bengal in 2010. He joined as PhD scholar in the department of Computer Science & Engineering in IIT Kharagpur in June 2010. His research interests lie in the areas of Algorithms, Cryptography and Computational Number Theory.*

***Supervisor: Prof. Abhijit Das***

## Batch Verification of Standard ECDSA Signatures

Currently, we are working on an old problem of *Signature Schemes* in Public-Key Cryptography. We are trying to verify multiple *Digital Signatures* in batches, especially *Elliptic Curve Digital Signatures*. We proposed an algorithm which is based upon the naive idea of taking square roots in the underlying field. We proposed three new algorithms which replace square-root computations by symbolic manipulations or resultant computations to improve the efficiency. We did experiments on NIST prime curves to measure the speedups. We obtained a maximum speedup of above seven over individual verification if all the signatures in the batch belong to the same signer and a maximum speedup of about two if the signatures in the batch belong to different signers. These algorithms are practical only for small ($\leq 10$) batch sizes. We also port our algorithms to the NIST Koblitz curves defined over fields of characteristic 2, and Edwards curves.

**Sandip Karmakar**
Email: sandip1kk@gmail.com
Joined the department in: December 2010

***Sandip Karmakar*** *received his B.E. degree in Computer Science & Technology from Bengal Engineering and Science University, Howrah, WB in 2004. After receiving his B.E., he worked in Software Industries from June 2004 to December 2007. Since May 2008, he has been a research scholar in the department of Computer Science & Engineering in IIT Kharagpur. He received M.S. (by Research) from CSE of IIT Kharagpur in Oct 2010. Since Dec 2010, he is working towards his PhD degree in the same department. His research interests are in the areas of Cryptography, Cellular Automata and VLSI.*

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

## Cryptanalysis and Design of Stream Ciphers

My broad area of research is *cryptanalysis and design of stream ciphers*. We are mainly working in *scan-based side channel attacks* and *fault attacks* on stream ciphers, both of which are *side channel attacks*. Another area of cryptanalysis we are currently working on is the algebraic cryptanalysis method *cube attack*. Our research also involves *design of cellular automata based stream ciphers*.

Scan chain based attacks are a kind of side channel attack, which targets one of the most important features of today's hardware - the test circuitry. Design for Testability (DFT) is a design technique that adds certain testability features to a hardware design. On the other hand, this very feature opens up a side channel for cryptanalysis, rendering crypto-devices vulnerable to scan-based attack. We have shown that the eStream ciphers, Trivium and Grain-128 can be analyzed using scan based side channel attack in a few minutes. We have proposed a more generalized approach which may break any cryptographic algorithm through scan chain interface in not more than few minutes and demonstrated it on hardware based eStream ciphers, Trivium, Grain-128, MICKEY 2-128. We also proposed a countermeasure to prevent such kind of attacks on stream ciphers.

Fault attacks are one of the most efficient form of side channel attack against implementations of cryptographic algorithms. In this attack, faults are injected during cipher operations. The attacker then analyzes the fault free and faulty cipher-texts or key-streams to deduce partial or full value of the secret key. The literature shows that both the block ciphers and stream ciphers are analyzable using fault attack. We have shown that the eStream cipher Grain-128 can be attacked by inducing faults in the NFSR. The attack requires about 56 fault injections for NFSR and a computational complexity of about $2^{21}$, hence, it can be performed practically. Currently, we are working on multi-bit fault attacks on eStream ciphers and prevention of such kind of attacks.

Cube attack was introduced by Ita Dinur and Adi Shamir in Eurocrypt 2009. It is a kind of high order differential attack. The main challenge in this kind of attacks is finding cubes. We have proposed a heuristic to find cubes which was successfully applied to a simplified version of Trivium in less than 5 hours. Currently we are working on improving the existing results on Trivium using cube attacks and trying to apply cube attacks on other ciphers. Another area of cube attack that we are working on is the hardware implementation of cube attack, cube testers and dynamic cube attack. The hardware is to be designed to perform the mentioned attacks, distinguishers on state of the art stream ciphers.

The final area of our current research is the design of stream ciphers. During our previous research on design of stream ciphers using Cellular Automata we identified certain hybrid CA configurations that are cryptographically suitable. In the ongoing research, we have proposed cryptographic stream ciphers using the identified Cellular Automata configurations. We are now working on design of a stream cipher using Cellular Automata which is based on the hybrid cellular automata and provides high speed, achieves low power and cryptographic efficiency.

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

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

***Supervisors: Prof. Animesh Mukherjee and 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.

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

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

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

## On Some Digital-geometric Applications of Farey Sequence

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

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

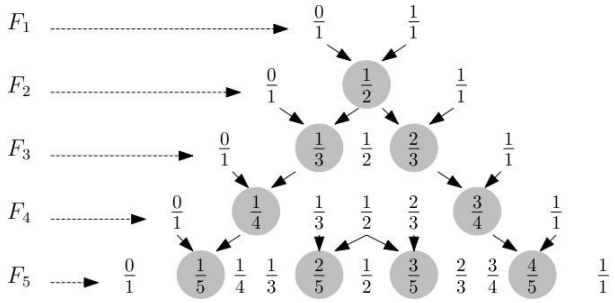
**Polygonal approximation:** An efficient boundary representation of an object in the digital plane is done through polygonal approximation. During approximation, "reasonably collinear" straight edges are successively merged. The collinearity is tested by edge slope, which corresponds to AFT rank. If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

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

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

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

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




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

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

**References**


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

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

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

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

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

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

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

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

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

## Impact of Micro-architecture on Side-channel Attacks

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

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

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

***Supervisor: Prof. Soumyajit Dey***

## Early Analysis of System Reliability using Probabilistic Program Models

The reliability of a system is increasingly being considered as a first class criteria in the design space of mission critical as well as soft real-time systems. However, automated synthesis and verification tool flows for such reliable embedded systems are still in their infancy. However, a criticism of such works would be that the granularity of the analysis is (un)fairly coarse grained. We propose a fine grained (and hence more accurate) reliability analysis method by considering reliability in all steps of the embedded system tool flow.

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.

Our work proposes probabilistic programs as initial models for functional modeling of reliable systems. We plan to build formal analysis methods for validating such models and leveraging model checkers and theorem provers for counter example based refinement of probabilistic programs. A subsequent step is integrating such analyses into synthesis tools for embedded system design.

We expect that the proposed work shall be beneficial in providing higher assurance in the design flow of reliable systems using the rigor of formal analysis methods.

**Shyantani Maiti**
Email: shyantani.maiti@gmail.com
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 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.*

***Supervisor: Prof. Pralay Mitra***

**Soma Saha**
Email: somasaha@cse.iitkgp.ernet.in
Joined the department in: July 2009

***Supervisor: Prof. Rajeev Kumar***

***Soma Saha*** *received a B.Tech. degree in Computer Science & Engineering from University College of Science & Technology, University of Calcutta, Kolkata in 2007, and an M.Tech. degree in Computer Science & Engineering from University College of Science & Technology, University of Calcutta, Kolkata in 2009. From July 2007 till 14th July 2009, she was attached with Maharaja Manindra Chandra College, University of Calcutta, Kolkata, as a Guest Lecturer in Department of Computer Science. Since 22nd July 2009, she has been a research scholar in the department of Computer Science & Engineering in IIT Kharagpur. Her research interests are in the areas of multi-objective combinatorial optimization and evolutionary programming.*

## Unifying Heuristics and Evolutionary Computing to Characterize and Solve Certain Combinatorial Optimization Problems

Multi-objective combinatorial optimization (MOCO) problems play a crucial role in many engineering applications. However, the existence of multiple conflicting objectives and therefore multiple feasible solutions in MOCO problems increases the difficulty to solve them. In this research work, in an attempt to yield quality solutions across the complete range of the Pareto fronts, we unify existing heuristics and propose problem-specific multi-objective evolutionary algorithm (MOEA) frameworks for solving the bi-objective minimum spanning tree (BOMST) problem, bi-objective graph coloring problem (BOGCP). We also consider constraint satisfaction problems (CSPs) along with MOCO problems because combinatorial search methods can be used to solve them due to complex and combinatorial nature of most of the CSPs.

### References

[1] K. Deb, Multi-Objective Optimization using Evolutionary Algorithms. John Wiley & Sons, Chichester, 2001.

[2] A. Singh and A.K. Gupta, “Improved heuristics for the bounded diameter minimum spanning tree problem”, Journal of Soft Computing, 11: 911-921, 2007.

[3] P. Galinier and J. K. Hao, “Hybrid evolutionary algorithms for graph coloring”, Journal of Combinatorial Optimization 3 (4): 379–397, 1999.

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

***Soumajit Pramanik*** *received his B.Tech degree in Computer Science and Engineering from WBUT in 2011, and M.Tech degree in Computer Science from Indian Statistical Institute, Kolkata, in 2013. His PhD research topic is interdependent networks.*

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

Today's networks are becoming increasingly dependent on one another. Nodes in interacting networks can be interdependent, and in this case the function or activity of a node in one network depends on the activity of the linked nodes in another network. Diverse real-world infrastructural networks such as communication systems, water supply, transportation, fuel and power stations are coupled together. Although investigations of the different network dynamics of complex networks have triggered enormous interest and debate, still most of the recent works have focused on each single, isolated network where no interaction with other networks is considered. My Ph.D. research mainly focuses on understanding the effects of different dynamical processes (growth, spread, breakdown etc.) on interconnected coupled networks which behave quite differently from isolated networks. With the insight gathered from that study, I also try to observe the effects of such dynamics on some real-world complex interconnected networks.

**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.

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

***Sourav Kumar Dandapat*** *received a B.E. degree in Computer Science from Jadavpur University in 2002 and an M.Tech. degree in Computer Science from IIT Kharagpur in 2005. From July 2005 till November2007, he worked in IBM ISL, Bangalore, as a System Software Engineer. From December 2007 till February 2009, he worked in Magma Design Automation, Bangalore, as an associate member of technical staff. Since July 2009, he has been a research scholar at the department of Computer Science and Engineering in IIT Kharagpur. His research interests are in the areas of Wireless Internet.*

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

## Association control scheme for wireless mobile environment

Wireless clients associate to a specific Access Point (AP) to communicate over the Internet. Current association methods are based on maximum Received Signal Strength Index (RSSI), implying that a client associates to the AP with the strongest signal around it. The main drawback in RSSI based technology is that the global parameters are not considered during association, hence effective strategy to handle skewed geographical distribution of devices (thereby ensuring fairness) cannot be devised. However, in today's enterprise WLANs, multiple APs are getting connected to a central controller through a high speed wired backbone. As a result, modern networks are becoming semi-centralized through hybrid wired-wireless architecture that offers new opportunities to redesign protocols for future wireless. Hence, there is a need to develop smart association control schemes which will ensure higher admission along with fairness, exploiting the global view of the APs. This is particularly pronounced in light of enterprise WLANs shifting to the single wide-channel mode (proposed by Meru Networks) to reduce the problems of interference management and frequent handoff. Association control is likely to play a key role in such environments. So, the broad objectives of our research can be summarized as follows – (a) Develop an AP-guided association control strategy that exploits the global view of APs for association decision. and (b) Maximize the number of connections admitted while maintaining fairness in bandwidth allocation.

## Distributed Content Storage for Just-in-Time Streaming

Uninterrupted streaming on the fly is an interesting issue of research in last few years. Due to low data rate, high congestion, it becomes almost impossible to deliver streaming data to users on the fly in uninterrupted fashion. Municipal WiFi networks open up a new opportunity. External memory can be easily hooked up with Access Pointi(AP) to cache popular contents, so that when request for popular contents arrives it is served locally. However, there is a limit in the amount of memory added with an AP. A single AP would not be able to cache good number of popular files. If we can find out a content distribution strategy over municipal WiFi networks where APs of WIFi networks collaboratively cache popular contents then we can serve more requests. Collaborative caching strategy should take care of uninterrupted streaming on the fly.

## Authentication Using User's Daily Activity

A user maintains 26 accounts on an average. It is quite unlikely that any user can maintain separate passwords for all these accounts. This boils down to bad habit of keeping similar passwords which are also most likely derivable from common passwords, their online social information. These facts make user's security vulnerable. Biometric, which is state of the art in security, is not always feasible. This motivates us to find some easy solution of this classical problem. User's daily activities do have a unique signature and lots of those activities can be electronically logged. In this proposed scheme information regarding different activities is used as challenge for accessing any system or application.

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

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

***Supervisor: Prof. Jayanta Mukhopadhyay***

## Computational Modeling of Phylogenetic Evolution

Phylogenetic trees represent evolutionary relationships between 'taxa' (entities such as genes, populations, species, etc.) using a tree structure. Every leaf of the tree uniquely represent one taxon. The tree can be rooted or unrooted. All the internal (non-leaf) nodes have a degree of 3. Given multiple gene (DNA) or protein sequences of different taxa as input, standard phylogeny reconstruction methods first estimate the distance (i.e. dissimilarity) between individual pairs of taxa, by computing the difference between corresponding DNA or protein sequences using sequence alignment and specific distance correction methods (such as Jukes-Cantor, Kimura models) [1, 2]. Lower distance between a pair of taxa indicates that, evolutionarily they are closely related (derived from a common ancestor, which is very recent with respect to the overall tree hierarchy). There are four main approaches to construct phylogenetic trees, based on either: 1) distance matrix, or 2) maximum likelihood, or 3) maximum parsimony, or 4) Bayesian reconstruction [1, 2]. Our focus lies in the distance based phylogenetic reconstruction. Calculated distance values between individual pairs of taxa are arranged in the form of a distance matrix, which is then used to derive a tree that approximates the computed distance values as closely as possible.

A distance matrix is *additive* [2], if distance between every taxa pair (located in two leaves of the tree) can be exactly reflected in the tree branches between them. In other words, sum of tree branch lengths between the taxa pair is exactly equal to the estimated distance measure between them. For an additive distance matrix, reconstruction of phylogenetic tree from the matrix is trivial and requires $O(N^2)$ (N = number of input taxa) operations. Obtaining an additive distance matrix for input set of taxa requires knowledge of exact number of mutation or evolutionary changes along each edge of the phylogenetic tree. Such accurate distance measure for individual taxa pairs is often not possible to obtain in real biological datasets. With non additive input matrix, construction of phylogenetic tree is performed using alternative approximation algorithms, of which the most widely used is the Neighbor-Joining (NJ) approach [3]. The method is based on clustering a pair of taxa using their proximity as well as their mutual separation to other taxa. The algorithm has a time complexity of $O(N^3)$, and it is highly accurate in terms of producing the phylogenetic tree topologically close to the ideal one, especially for small values of N. Faster approximations of NJ algorithm often compromises its accuracy, especially for datasets involving large taxa set. Our research focuses on preprocessing the input non-additive matrix such that various sub-matrices of the input matrix exhibit *additive* property. Complete conversion of a non-additive matrix to an additive one is a NP complete problem. So, our focus is to alter the elements of original matrix to obtain additive sub-matrices, or in general, partially additive matrix. Greedy heuristics are employed to restrict the changes in the input matrix as low as

possible. NJ algorithm, with the input of such modified partial additive matrix, reconstructs more accurate phylogenetic trees, as experimented in various datasets.

However, NJ based phylogenetic reconstruction for a large set of taxa requires estimation of distances between each pair of taxa, using input protein or DNA sequences. However, such pairwise distance estimation is not feasible for large taxa set. Another solution is to build small or moderate phylogenetic trees using NJ (or other phylogenetic reconstruction methods) for a set of overlapping taxa subsets, thus creating a set of input phylogenetic trees having overlapping (complete or partial) set of taxa. Finally, individual trees are synthesized to form a *Supertree* [4] depicting the evolutionary relationships between complete taxa set of the input trees. However, input trees (even with same taxa set) can be individually constructed using different DNA or protein sequences, or using different phylogenetic reconstruction methods. So, relationships between individual taxa pairs can produce conflicts among the source trees itself. Ideally a *Supertree* needs to select the consensus relationships among all taxa pairs. Implementation of such consensus tree is NP-hard, and a *strict consensus tree* excluding all conflict cases [4], select a subset of complete input taxa set. Current research focuses on a *Supertree* construction algorithm using the complete input taxa set, such that the consensus relations are selected as much as possible, using a greedy heuristic. During *Supertree* construction, the method applies relationships between individual taxa pairs as per the configuration of input source trees, and whether such relation does not induce a conflict to the current supertree. For biological datasets, there is no model supertree for benchmarking the accuracy of the supertree. So, the performance is measured based on topological distance of individual source trees to the output supertree (pruned with respect to the taxa set of corresponding input source tree). The performance of our method is found to be better or equal compared to the existing studies, with respect to different performance measures. Moreover, suggested method involves considerable lower time and space complexity than reference approaches, thus suitable for application in large biological datasets.

**References**


[1] N.C. Jones and P.A. Pevzner, An Introduction to Bioinformatics Algorithms (Computational Molecular Biology). The MIT Press, 2004.

[2] J. Felsenstein, Inferring phylogenies. Sinauer Associates, 2003.

[3] N. Saitou and M. Nei, “The neighbor-joining method: a new method for reconstructing phylogenetic trees.,” Mol Biol Evol., vol. 4, no. 4, pp. 406–25, 1987.

[4] M.S. Swenson, R. Suri, C. R. Linder, and T. Warnow, “Superfine: Fast and accurate supertree estimation,” Syst Biol, vol. 61, pp. 1–14, 2011.

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

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

***Supervisor: Prof. Indranil Sengupta***

## Some topics in RFID Communication

RFID technology helps to identify an object efficiently. In this technology, the reader reads the identification information from RFID tag which is attached to an object and based on that information it identify that object. Moreover, the attachment of multiple number of tags in an object increases the detection probability in comparison to single tag. The communication to identify the object has many security and privacy risks and since the RFID tags are very low cost device they suffer from resource constraint problem. Therefore the communication process needs to be lightweight and adequately secure. An object needs to be identified for various reason. Our focus is on object authentication, object searching and object binding. In object authentication problem, we propose two protocols which can efficiently authenticate and hence identify an object. The owner of a set of objects may search for a particular object. Therefore we propose an object searching protocol which can efficiently search the require object. In object binding problem, there is a need to generate a proof of coexistence of a set of relevant objects. A set of objects may involved in execution of an event and the proof of coexistence helps to avoid wrong execution of that event. We propose an object binding protocol which can generate a concrete proof of coexistence of a set of relevant objects. We have designed all the protocols which can be applicable in multi-tag arrangement and can fulfill most of the security requirements in RFID communication.

**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 Systems Incorporation. Since January 2014 he has been a research scholar in the department of Computer Science and Engineering. His research interests are inthe areas of Distributed Systems.*

***Supervisor: Prof. Arobinda Gupta***

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

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

***Supervisor: Prof. Dipankar Sarkar***

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

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

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

**Sudipta Saha**
Email: sudipta.saha.22@gmail.com
Joined the department in: July 2010

***Sudipta Saha*** *received B. E. degree in Computer Science & Technology, from Bengal Engineering College (at present known as Bengal Engineering and Science University), Shibpore in 2002 and MTech degree from Indian Institute of Technology (IIT), Kharagpur in 2008. He worked as 'Senior Lecturer' in a college affiliated under West Bengal University of Technology (WBUT). He also served as 'Associate Member of Technical Staff' in Magma Design Automation Pvt. Ltd., Noida. In 2008, he joined PowerSys Technologies Pvt. Ltd., a start up organization established by two senior faculty members of IIT Kharagpur. Since July 2010, he has been a research scholar in the department of Computer Science & Engineering, IIT Kharagpur. His research interests are in the areas of Computer Network and Bioinformatics.*

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

## Dissemination dynamics in large scale decentralized systems: structural and functional analysis

Diffusion of any quickly and infinitely replicable entity such as information, idea, emotion etc., is a significant aspect of any large scale distributed system such as technological communication systems, social systems etc. In some cases, engineers design sophisticated algorithms for disseminating a given piece of information in the system, while in other cases, the percolation of information gets executed silently in a more autonomous fashion and comes into visibility when it results in a mass change. In this research, through extensive computer simulations as well as using mathematical models we analyze different types of such spreading processes taking place in few different kinds of networks. In some cases we do algorithmic and process oriented analysis and in the other cases, we form a hypothetical network structure which governs the dissemination process and perform a thorough analysis of that structure. Moreover, we identify that, in all these kinds of spreading processes, there are various kinds of constraints present in various forms which mainly resist the flow of information through the links. One of the primary aims of these analyses is to identify these constraints and understand their effects by modeling them as system parameters.

As an instance, one of the most desirable features of the dissemination services, implemented on large scale peer-to-peer (technological) communication systems is the maximization of the coverage, i.e., the number of distinctly visited nodes under constraints of network resources as well as time. However, redundant visits of nodes by different message packets (modeled, e.g., as walkers) initiated by the underlying algorithms for these services, cause wastage of network resources. Through a detailed functional analysis of the multiple random walker based dissemination algorithms we identify that redundancy quickly increases with increase in the concentration of the walkers. Based on this postulate, we design a very simple distributed algorithm which dynamically estimates the concentration and thereby carefully proliferates walkers in sparse regions. We test our algorithm in various kinds of network topologies whereby we find it to be performing particularly well in networks that are highly clustered as well as sparse.

On the other hand, we also identify that the dissemination of idea, information, emotion etc., through human contact networks are significantly influenced by many issues related to the social

behavior of humans, specifically their tendency of selective visits to different places, choice, habits and mobility patterns etc. These aspects primarily regulate the interactions among humans in an indirect fashion. We identify that these complex interactions among the humans, result in a special network structure which evolves with time and controls the flow of the information in the system. We use two graph theoretic concepts - 'Alphabetic bipartite network' and 'Random threshold graph' to model this special network structure and employ statistical techniques to analyze its structural properties. Later, we apply these developed theories to analyze few specific networks such as 'Intergroup Network' (a form of social network) and 'Delay Tolerant Network' (a form of peer-to-peer communication networks). Moreover, in this research we also identify that the spread of pathogenic organisms get a big advantage due to the indirect communications among the humans in the system. Therefore, as a related task, we also do a thorough analysis of the actual process of this indirect spreading through a discrete dynamical system based SIS model.

**Suman Kalyan Maity**
Email: sumankalyannit@gmail.com
Joined the department in: July 2013

***Suman Kalyan Maity*** *has received a B.Tech. degree in Computer Science & Engineering from National Institute of Technology, Durgapur in 2011. He has completed his M.S in Computer Science & Engineering from Indian Institute of Technology, Kharagpur in 2014. Since July 2013, he has been a PhD research scholar in the department of Computer Science & Engineering in IIT Kharagpur. His research interests are in the areas of Complex Systems and Language Dynamics.*

***Supervisor: Prof. Animesh Mukherjee***

## Aspects of opinion formation in social networks

Opinion formation is an important phenomena in social group dynamics. We live in a world where everyday we come across many situations in which it is necessary for a group to reach shared decisions. Agreement makes a position stronger, and increases its impact on society. From a vast repertoire of models in literature, we choose naming game as an opinion formation model. This agent-based model captures the essential features of the agreement dynamics by means of a series of memory-based negotiation process.

We analyze various aspects of social group dynamics like the impact of underlying societal structure and the effect of various social factors on the naming game dynamics. Our first objective is to observe the impact of time-varying properties of the social network of the agents on the naming game. We find that networks with strong community structure hinder the system from reaching global agreement; the evolution of the naming game in these networks maintains clusters of coexisting opinions indefinitely leading to metastability. Further, we investigate the dynamics in perfect synchronization with an evolving social network shedding new light on the basic emergent properties of the game that differs largely from what is reported in the existing literature.

As a following objective, we then analyze the impact of social factors on the game dynamics. We observe that presence of dominant opinions in the system leads to faster agreement. We also identify how the presence of a rigid minority of agents can lead to the emergence of dominant opinions.

We analyze the impact of resistance toward learning on the naming game dynamics and observe that there exist a non-trivial consensus-polarization phase transition and for almost all social network topology, we observe that beyond the critical value of the parameter $\alpha$ describing the inflexibility toward learning, the number of unique words increase manifold in the system and hence the time to consensus diverges possibly pointing to an universal aspect of language learning.

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

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

***Supervisor: Prof. Pallab Dasgupta***

**Formal Verification on Embedded System Software 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 formalisms 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.

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

***Sumanta Pyne*** *received a B.Tech. degree in Computer Science from Meghnad Saha Institute of Technology, Kolkata in 2005, and an M.E. degree in Computer Science from Bengal Engineering and Science University, Shibpur in 2009. From July 2005 till January 2006, he worked in Hi-Q Solutions, Kolkata, as a programmer. From January 2006 till June 2007 he was a lecturer at Techno India College of Technology, Kolkata. Since December 2009, he has been a research scholar in the department of Computer Science & Engineering in IIT Kharagpur. His research interests are in the areas of Power Aware Software.*

***Supervisor: Prof. Ajit Pal***

## Power Aware Software

It has been observed that power reduction can be achieved at a higher degree at higher level i.e. at algorithmic level than at circuit and gate level. In past decades of CMOS technology dynamic power dissipation dominated the leakage power. As CMOS technology is reducing in dimensions leakage power is gradually becoming a challenge for power awareness. In addition to low power circuits, it is necessary for the system software like compilers and operating systems to be well equipped to achieve low power. Modern processors run on multiple voltage-frequecy pairs. Multicore processors have evolved keeping power and thermal management in mind. These have provided a room for designing low power software.

Compilers should deal with code optimization techniques to reduce power consumption of program. Early research on code optimization focused on time and space. Some of them reduce power consumption while others like software prefetching increases power consumption. We have proposed a scheme for power-aware software prefetching, where the software prefetching program trades performance for low power dissipation on an Xscale processor. Branch Target Buffer (BTB) plays an important role for pipelined processors in branch prediction during the execution of loops, if-then-else, call-return, and multiway branch statements. It has been observed that 20% of instructions in a program are related to branch. Access to BTB consumes 10% of total energy consumption of a program in execution. We introduced the use of *K-d* tree and pattern matcher to generate efficient code, i.e., lesser execution time as well as lesser energy, for multiway branch. However, instead of enhancing performance, Voltage Frequency Scaling (VFS) can be applied to achieve more energy saving without degradation in performance. This work is evaluated on a wide range of benchmark programs. The BTB energy saving in this work lies in the range 20% to 80% with small improvement performance as well. The total energy reduction is in the range 3-12%.
We are working on compiler optimization techniques to minimize both dynamic power and leakage power consumption.

Operating Systems should care process, memory, I/O and file management to achieve low power. Achieving low power is challenging for real time systems as it may degrade performance. Power and thermal aware task scheduling for multi-processors/multi-core processors is an important area of our research. As, multi-processor task scheduling is an NP-complete problem. Sophisticated

battery enabled systems require task scheduling techniques that will elongate the battery lifetime. We are also working on power-aware memory management techniques for garbage collection of Kilobyte Virtual Machine (KVM), the Java Virtual Machine (JVM) for Java enabled embedded systems.

There is a lot of scope in designing software for low power in different domains of computer science. Some of them are Database Management System and Computer Networks. As both of them is the most important part of today's industry. Power aware database query optimization is an area of our concern. Network protocols right from data link layer to application layer should be power-aware because most of today's hand-held devices provide networking facilities.

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

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

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

## Community Identification in Large Scale Networks

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

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

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

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

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

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

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

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

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

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

Many tasks would be revolutionized if machine could automatically interpret the human activities as performed in our day to day life. Hence human motion tracking and activity analysis has been a highly active research area in computer vision. These are widely applicable to various domains, such as security surveillance in public spaces, Human-Computer/Robot Interaction (HCI/HRI), video retrieval, virtual reality, computer gaming, and many other fields.

Recent technological advances have led to the development of novel yet affordable depth cameras like Kinect, that can acquire dense, two and half dimensional scans of a scene in real-time. Such depth images are hardly dependent of lighting conditions and variations in visual appearance due to clothing. Beside depth sensing, it also detects and tracks different human body motions by using the 20-joints human skeletal model.

Like most sensors Kinect also has limitations. The quality of depth images often suffer from limited accuracy and stability due to depth holes and inconsistent depth values. Depth holes may occur in a depth image on the boundary of objects, in smooth and shiny surfaces, and in other scattered locations. Additionally, the depth of a particular pixel often keeps on changing from one frame to the next, even when the scene is static. Kinect's field of view is $43^0$ in vertical and $57^0$ in horizontal directions. Hence a full human figure is visible only when it is about 3m away which is very close to the maximum depth range of 3.5m. Further, Kinect has only a uni-directional vision of objects or people. It needs to be moved around the subject to capture the opposite side. Two or more Kinects can be used simultaneously to overcome these limitations. Unfortunately, when more than one Kinects are used for a scene, their IR patterns often overlap and interfere with each other. This shows up as blind spots or holes (zero depth) in the depth map in the overlapping area. Interfering IR also increases instability and results in vibrating depth values even for static points. These are known as IR Interference Noise (IR Noise).

We have started our work with noise characterization. We characterize the noise [1] in Kinect depth images based on multiple factors and introduce a uniform nomenclature for the types of noise. This characterization would help to selectively eliminate noise from depth images either by de-noise filtering or by adopting to appropriate methodologies for image capture. Next, we explore deeper

on mitigating interference noise for increasing field of view with multiple Kinects [2]. Further, we try to use mirror/s to get 3D view of an object. Initially, we estimate the distance and the orientation of a mirror from the camera [3]. These parameters will help to solve the geometry for 3D reconstruction.

The objective of our research is to effectively exploit the potential of the Kinect sensor for 3D reconstruction in general and human motion tracking, movement representation and activity analysis in particular.

**References**


[1] Tanwi Mallick, Partha Pratim Das and Arun Kumar Majumdar, *Characterizations of Noise in Kinect Depth Images*, IEEE Sensor Journal, Accepted for publication, 2014.

[2] Tanwi Mallick, Partha Pratim Das and Arun Kumar Majumdar, *Study of Interference Noise in Multi-Kinect Set-up*, Proceedings of International Conference on Computer Vision Theory and Applications, VISAPP 2014, Lisbon, Portugal, 173–178, 2014.

[3] Tanwi Mallick, Partha Pratim Das and Arun Kumar Majumdar, *Estimation of the orientation and distance of a mirror from Kinect depth data*, Proceedings National Conference on Computer Vision, Pattern Recognition, Image Processing and Graphics NCVPRIPG 2013, Jodhpur, India, 2013. Proceedings is being published by IEEE and will be available online on IEEE explore.

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

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

***Supervisor: Prof. Sudebkumar Prasant Pal***

## Bicoloring Cover for *k*-Uniform Hypergraphs

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

This problem can be mapped to a set of bicolorings of a $k$-uniform hypergraph $G(V, S)$, $|V| = n$, $|S| = m$, with the doctors representing the vertices, the groups being the $k$-uniform hyperedges, and the task assigned to the doctors being a bicoloring of the vertices. The minimum number of shifts required is the minimum size of the set of bicolorings. We define Bicoloring Cover number $\chi_c$ as the minimum number of bicolorings required such that every hyperedge is properly bicolored (that is, non-monochromatic) in some bicoloring. Formally, let $G(V, S)$ be a hypergraph with vertex set $V$, $|V| = n$, and hyperedge set $S$. Also let $X$ be a set of bicolorings $\{X_1, X_2, \ldots, X_n\}$. The dependency of any hyperedge $S_i$ is the size of the set $\tau(S_i)$ of hyperedges such that each hyperedge in the set shares at least one vertex with $S_i$ . Then, $X$ is a bicoloring cover for $G$ if $\forall e \in S$, $\exists X_i$ such that $e$ is non-monochromatic with $X_i$. The minimum cardinality of all such $X$'s is called the Bicoloring Cover number $\chi_c(G)$.

Our current line of research focuses on characterizing the relationship between the number of hyperedges $|E|$, the dependency of any hyperedge $d$ and $\chi_c(G)$. Our objective is to design polynomial-time algorithms for finding bicoloring covers that are of sizes close to $\chi_c(G)$.

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

***Supervisor: Prof. Anupam Basu***

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

## Toward a Computational Model for the Organization and Access of Bangla Polymorphemic Words in the Mental Lexicon

Understanding the organization of the *mental lexicon* is one of the important goals of cognitive science. *Mental lexicon* refers to the representation of the words in the human mind and the various associations between them that help fast retrieval and comprehension of the words in a given context. Words are known to be associated with each other at various levels of linguistic structures namely, orthography, phonology, morphology and semantics. However, the precise nature of these relations and their interactions are unknown and very much a subject of research in psycholinguistics. A clear understanding of these phenomena will not only further our knowledge of how the human brain processes language, but also help in developing apt pedagogical strategies and find applications in natural language processing.

One of the key questions that psycholinguists have been investigating for a long time and debating a lot about is the mental representation and access mechanisms of polymorphemic words: whether they are represented as a whole in the brain or are understood by decomposing them into their constituent morphemes. That is to say, whether a word such as "*unimaginable*" is stored in the mental lexicon as a whole word or do we break it up "*un-*" , "*imagine*" and "*-able*", understand the meaning of each of these constituent and then recombine the units to comprehend the whole word. Such questions are typically answered by designing appropriate priming experiments or other lexical decision tasks. The reaction time of the subjects for recognizing various lexical items under appropriate conditioning reveals important facts about their organization in the brain.

There is a rich literature on organization and lexical access of polymorphemic words where experiments have been conducted mainly for English, but also Hebrew, Italian, French, Dutch, and few other languages (Frost et al., 1997; Marslen-Wilson et al. 1994). However, we do not know of any such investigations for Indian languages, which are morphologically richer than many of their Indo-European cousins. On the other hand, several cross-linguistic experiments indicate that mental representation and processing of polymorphemic words are not quite language independent (Taft, 2004). Therefore, the findings from experiments in one language cannot be generalized to all languages making it important to conduct similar experimentations in other languages. Bangla, in particular, features stacking of inflectional suffixes (e.g., *chhele* + *TA* + *ke* + *i* "to this boy only"), a rich derivational morphology inherited from Sanskrit and some borrowed from Persian and English, an abundance of compounding, and mild agglutination.

The primary objective of this research is to understand the organization of the Bangla mental lexicon at the level of *morphology*. Our aim is to determine whether the mental lexicon decomposes morphologically complex words into its constituent morphemes or does it represent the unanalyzed surface form of a word. We apply the cross modal repetition priming technique to answer this question specifically for derivationally suffixed polymorphemic words of Bangla. We observe that morphological relatedness between lexical items triggers a significant priming effect, even when the forms are phonologically unrelated. On the other hand, phonologically related but morphologically unrelated word pairs hardly exhibit any priming effect. These observations are similar to those reported for English and indicate that derivationally suffixed words in Bangla are accessed through decomposition of the word into its constituent morphemes.

Further analysis of the reaction time and error rates per word and per subject reveal several interesting facts such as (a) apart from usage frequency, word length and presence of certain orthographical features also affect the recognition time of a word, and (b) certain derivational suffixes inherited from Sanskrit, which usually make the derived word phonologically or semantically opaque, do not trigger priming; this indicates that these morphological relations are no longer recognized or internalized by the modern Bangla speakers. These and similar other observations make us believe that understanding the precise nature of the mental representation of morphological processes in Bangla (as well as other Indian languages) is a challenging and potent research area that is very little explored.

**References**

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

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

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

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

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

## Analysis and Visualization of emerging global gene expression patterns in Microarray data using Unsupervised learning

Although the human genome sequencing project is almost over, the analysis has just begun. DNA microarray technologies provide gene expression data on a massive scale. DNA microarrays are ordered samples of DNA placed in high density on a solid support such that each sample represents a particular gene. Thus can track the global expression levels of thousands of genes simultaneously and can reveal large amount of data about the inner life of a cell. Examples of some possible comparisons are (1) cells before and after drug treatments (2) tissues from young vs. old age (3) healthy vs. cancerous tissues (4) yeast used in fermentation for beer vs. yeast used in fermentation for wine. Microarray based study of global gene expression patterns is often used to appreciate differential behaviour of various stages of tumorigenesis. Thus many important biological, physiological, medical, and industrial phenomena can be studied using the arrays. The challenge is to evaluate these huge data streams and extract useful information.

Given a series of microarray experiments for a specific tissue under different conditions our aim is to find genes which are more informative or are signature genes that robustly distinguish different structures present in the data. The objective is to provide a data analysis methodology for extraction and visualization of such structure patterns in global gene expression during progression of a disease. The genes are our features that have the biggest impact on describing the results. Noisy or irrelevant attributes make the classification or clustering task more complicated, as they can contain random correlation. Our aim is to filter out these features. When class labels of the data are assailable we use supervised feature selection, otherwise unsupervised feature selection is appropriate. Recently unsupervised feature selection has attracted a lot of attention especially in bioinformatics and text mining. Existing paradigms for the unsupervised analysis of gene expression data have focused on three important aspects: preprocessing and feature extraction from the data, clustering, and visualization. While the initial intent was to profile the expression patterns of individual genes with microarrays, the ability to cluster these patterns on a genome-wide scale and to access the pertinent genes in these emerging cluster patterns, has expanded the utility of microarrays to inferring the function of specific genes. Although the biological validation of hypotheses derived from microarray data remains necessary, the reliance on microarray generated data for individual gene information has risen to the forefront. On a larger scale, the analysis of many combined microarray data sets has taken this a step further to characterize more sophisticated biological phenomena such as cancer

development, and psychosocial effects. Such rapidly escalating complexity in gene expression data sets requires improved methods for both their analysis and visualization, if the data generated are going to be useful.

Our work focuses on explorative data analysis for finding the underlying structure from the global gene expression data, which may be multi-faceted by nature. The analysis of gene expression is followed by the ability to visualize, as a means of understanding the relationships between genes and the progression of the pattern structure. Detailed biological analysis of these underlying structures have potential for marker discovery, as well as development of novel treatment methodologies.

# MS Scholars

**Abhishek Chakraborty**
Email: abhishek_cky@yahoo.co.in
Joined the department in: December 2013

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

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

## Power attack vulnerability of stream ciphers

Encryption and decryption algorithms are used for secure and authorized exchange of information between a transmitter and a receiver over an insecure channel. Traditionally the robustness of cryptographic algorithms has been determined using mathematical models and statistical analysis. However the real life implementations of these cryptographic modules can be analyzed to launch Side Channel Attack (SCA), a major threat to the security robustness of the system executing the encryption.

There are several types of side channels through which information leaks inadvertently into the environment. The most prominent of them includes the measurement of power consumed or the time taken to perform a cryptographic function, the argument(s) to the function being the secret cryptographic key/data. A number of successful attacks using the above idea have been reported. Power attacks can be mounted by using some very standard test and measurement equipments that are widely available.The correlation between power consumption and the secret key dependent cryptographic operation can be analyzed to either directly mount an attack to reveal the key/data or be used in conjunction with a brute force attack to reduce the search space.

Stream ciphers are an important class of symmetric ciphers used extensively for encryption by many cryptosystems. They are popular because of their simplicity, efficiency and performance. The secure realization of stream ciphers is crucial to safeguard against SCAs. With this motivation, my current research work investigates the differential power analysis (DPA) attack vulnerability and it's countermeasure designs for various stream ciphers proposed in eSTREAM project.

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

***Abhrajit Sengupta*** *received his B.E. degree in Computer Science & Engineering from Jadavpur University, Kolkata in 2011. From June,2011 to April,2012 he worked as a member of Software Develoment Team at Acclaris Business Solutions Pvt. Ltd. He joined as an MS scholar in the department of Computer Science & Engineering in IIT Kharagpur in June 2012. His current research interests lie in the areas of Code Based Cryptography and design and implementation of some error-tolerant Message Authentication Schemes.*

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

## Design and Implementation of Error Tolerant Message Authentication Codes

There are two fundamental goals in cryptography, security and authentication. Message Authentication Code (MAC) helps achieving the later. It is a short piece of information, called tag, which serves as the authenticator, ensuring both data integrity and authenticity. A MAC algorithm sometimes called a keyed hash function is a symmetric-key method that accepts an arbitrary length message and a secret key as input and produces the MAC. This MAC value is then appended to the message, thereby preventing any unauthorized alteration by allowing the verifier(owner of the secret key) to detect any changes in the message. However, since physical transmission layers are noisy, channel noises are detrimental in authentication, causing the receiver to reject authentic messages. This problem can be solved by using MAC in conjunction with channel coding, which enables reliable delivery of digital data over unreliable or noisy channels. Thus, it is compelling to study some MAC construction techniques which are capable of correcting few errors that may occur during transmission. In our current work, we have focused on developing a suitable error-tolerant MAC scheme with a low cost architecture which can be implemented in common FPGA's.

**Anirban Ghose**
Email: anighose25@gmail.com, anirban.ghose@cse.iitkgp.ernet.in
Joined the department in: December 2013

***Anirban Ghose*** *received his B. Tech degree in Computer Science and Engineering from Heritage Institute of Technology, Kolkata in 2013. From September 2013, he has been working as a Research Consultant in the Department of Computer Science and Engineering, IIT Kharagpur under the project: "Architectural and Algorithmic Optimizations for Speech based communication interfaces in mobile devices." His areas of research interest include Program Analysis, High Performance Computer Architecture, and Machine Learning.*

***Supervisors: Prof. Soumyajit Dey and Prof. Pabitra Mitra***

## Machine Learning Assisted Formal Analysis of GPGPU Programs

Over the past decade, the processing power of the Graphics Processing Units (GPUs) has increased tremendously. Recent advances in the programmability of graphics cards have made it possible to leverage the computational power of GPUs for non-graphics based applications i.e. general-purpose computing on graphics processing units or GPGPU. With the rise of GPGPU programs, heterogeneous computing involving both GPU and CPU cores has become increasingly prevalent and attractive for mainstream programming. However, for a heterogeneous computing system to gain in terms of performance, automated identification of the nature of workload is necessary, i.e., whether a program part is *GPU or CPU friendly.* As it is today, this is a programmer's burden. Hence, the key challenge becomes mapping such program tasks to the right processing core in the system with the global objective of extracting optimal performance for the entire program.

We intend to use a machine learning based classification technique which may determine a good partition for a target program to be run on a GPGPU. The most widely adapted framework for heterogeneous computing is OpenCL, an open standard for parallel programming on GPGPUs. Static program analysis is performed on OpenCL programs to extract code features. Ensemble learning will be used to develop a model that will map features into partitions, i.e. classify the program tasks on the basis of code features to a particular partition across the heterogeneous system. Ensemble learning is a machine learning paradigm that uses multiple models to obtain predictive performance which is better than any of its constituent models. The goal is to use these ensemble techniques and test across a variety of existing benchmarks of OpenCL programs.

**Arnab Dhar**
Email: arnab832007@gmail.com
Joined the department in: December 2011

***Arnab Dhar*** *earned B.Sc. degree in Computer Science from Asutosh College, Kolkata in 2004, and MCA degree from RCC Institute of Information Technology, Kolkata in 2008. He worked in CVPRU, ISI, Kolkata, as a Project Linked Person for 2 years. Since July 2011, he has been working as a Junior Project Officer in ILMT project in IIT Kharagpur. He has joined in MS (by research) programme of Computer Science & Engineering Department, IIT Kharagpur, in January 2012. His research interests are in the areas of Computational Natural Language Processing.*

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

## Bangla Dependency Parser

Dependency parsing is the automatic analysis of the dependency relations in natural language sentences. The nodes of the parse tree represent the words and edges represent the dependency relations. There is a one to one correspondence between the parse tree and the sentence. Dependency relations are defined as the binary syntactic-semantic relations between the words. In recent years, Indian language dependency parsing gained a lot of attention and popularity. The parsers are used in almost all natural language applications like Machine translation, Summarization, Information retrieval, etc.

Dependency parsing can be broadly divided into grammar-driven and data-driven parsing. Many of the modern grammar-driven dependency parsers parse by satisfying the given set of constraints. Data-driven parsers, on the other hand, use a dependency tagged corpus (Treebank) to induce a probabilistic model for disambiguation. There are several statistical parsers available that can automatically create the model from the Treebank. However, some Bangla linguistic features like, Root, POS category, gender, number, person etc. should be used to observe their performance on Bangla parsing.

Building the dependency parser for a language like, Bangla is challenging due to its morphological richness and relatively free word order properties. The resource required for the Bangla dependency parsing is small as compared to English and European languages. Preparation of the comprehensive dependency relation set and the large sized Treebank for Bangla is still under construction.

**Ayan Palchaudhuri**
Email: ayan@cse.iitkgp.ernet.in, ayanpalchaudhuri@gmail.com
Joined the department in: December 2011

***Ayan Palchaudhuri*** *received a B.Tech. degree in Electronics and Communication Engineering from Birbhum Institute of Engineering and Technology in 2010. From February 2011, he worked as a Junior Project Assistant in the Department of Computer Science & Engineering, IIT Kharagpur, under the project : Hardware Security : Ensuring Trust in Integrated Circuits. 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 High Performance Integer Arithmetic Architectures for FPGAs.*

***Supervisor: Prof. Rajat Subhra Chakraborty***

## High Performance Integer Arithmetic Architectures for FPGAs

With significant increase in circuit complexity for FPGA based designs, even the most sophisticated CAD tools often output an inefficient technology mapped circuit with unsatisfactory performance and resource requirements. The designer under such cases needs to spell out directives and constraints to ensure high performance. Many integer arithmetic circuits, eg. adders, have sufficient modularity in their architecture, which is a pre-requisite for building FPGA-based efficient designs. The advantage extends even further when we realize circuits with higher order bit-widths by adopting the bit-sliced design paradigm, where an entire arithmetic circuit is built using identical modules of smaller bit width.

The regularity and modularity of the architectures lend themselves easily to design automation where a CAD software executable can be invoked from the design environment of the synthesis tool to realize efficient arithmetic circuits. The user will be prompted to specify the circuits or sub-circuits which may be a part of his larger system design and the tool will generate high performance circuit descriptions. These tools have the potential to be of high commercial value and will find numerous applications in developing hardware accelerators for signal and image processing algorithms and cryptography.

My research is primarily focused upon building efficient building blocks targeted towards the most popular FPGA families from Xilinx such as the Virtex-5 family. All our design approaches have realized circuits that can outperform the on-chip DSP slice based implementations, the Xilinx ISE GUI based circuit realizations or any other open-source arithmetic core generators for FPGAs.

**Debapriya Basu Roy**
Email: dbroy24@gmail.com
Joined the department in: December 2011

***Debapriya Basu Roy*** *received a B.Tech. degree in Electronics & Communication Engineering from RCC Institute of Information Technology, Kolkata in 2011. Since December 2011, he has been a research scholar in the department of Computer Science & Engineering in IIT Kharagpur. His research interests are in the areas of Cryptography and VLSI design.*

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

## FPGA Based Accelerators for Binary and Prime Field ECC and Their Side Channel Analysis

Field Programmable Gate Array (FPGA) is programmable integrated circuit which can be customized by the user according to his requirement. Due to its programmability feature, FPGA has gained lots of popularity in the fields like digital signal processing, cryptography, hardware-software co-design, ASIC prototyping, bio-informatics, computer hardware emulation etc. With the increase of sensitive information in the Internet, security is becoming a very important aspect of web applications. Cryptography provides a method for securing and authenticating the transmission of information over insecure channels. Elliptic curve cryptography (ECC) is a popular public key standard. It provides more security per bit compared to other security standards. Elliptic curve scalar multiplication, required by security protocol such as Transport Layer Security (TLS) and Internet Protocol Security (IPSec) is computationally intensive and creates performance bottlenecks for a number of applications involving web servers, cloud computing infrastructures, and data centers. FPGA accelerators for ECC can solve these problems. It can provide the necessary speeds to match the performance requirements of the application.

The hardware accelerators for ECC, though guarantees the speed up, it does not necessarily guarantee security against a side channel adversary. Side channel attack uses information gained from physical implementation of the cryptographic algorithm to break the security of the cryptosystem. The source of side channel information includes time, power, electromagnetic radiation, fault etc. Hence, though ECC has no theoretical weakness, its security against side channel attack depends upon the way it is implemented on hardware. Thus, proper evaluation of these algorithms against side channel attack is an absolute necessity.

Efficient implementation of ECC cryptosystem depends upon efficient implementation of underlying finite field arithmetic. Finite Field has many applications in the area of cryptography, number theory, coding theory. Finite Field arithmetic that is important to many cryptographic and error correcting applications involves working with Galois fields of type GF($2^m$). Multipliers which can support flexible input size are a crucial component of finite field processors. The present work targets efficient VLSI design of such variable size multipliers, operating on characteristic 2 field polynomials with degree varying to 512 bits. In order to optimize the area, and speed the design employs a sequential architecture, utilizing the Karatsuba-Ofman decomposition. The architecture reduces the critical path by designing an *overlap-free* variant of the original Karatsuba algorithm. Apart from

exploring wrt. the design parameters, namely levels and thresholding for Karatsuba multipliers, the present work also observes the effect of combinations of overlap free and naive Karatsuba multipliers on the overall area and speed. The results show that on a standard Virtex-4 platform, two levels of overlap free Karatsuba multipliers provides better area-time product and lesser computation delay. In the next work we aim to design a high speed, low area prime field multiplier using DSP blocks of the FPGA for high speed ECC scalar multiplication in GF(p).

High speed DSP blocks present in the modern FPGAs accelerate many computationally intensive applications. The DSP blocks can be used to implement prime field multiplication to accelerate Elliptic Curve scalar multiplication in prime fields. However, compared to logic slices, DSP blocks are scarce resources, hence its usage needs to be optimized. The asymmetric multiplier (25 × 18 signed multiplier), present in Virtex-5 and Virtex-6 FPGAs, opens a new paradigm for multiplier design. Due to these rectangular multipliers, decomposing the operands for multiplication becomes equivalent to a tiling problem. Previous literature has reported that for asymmetric multiplier, it is possible to generate a tiling (known as non-standard tiling) which requires less number of DSP blocks compared to standard tiling, generated by school book algorithm. In this work, we will provide a generic technique for construction of such tiling. The proposed technique can generate a tiling for multiplication of operands having arbitrary bit-width. We have generated this non-standard tiling for field multiplication in NIST specified curves and compared it with the school book algorithm to highlight the improvement in terms of speed.

SCA (Side Channel Attack) resistance strongly depends on the operating frequency due to RLC structure of a power grid. This property can potentially be exploited by an attacker to facilitate the attack by operating a device at favorable frequency. On the other hand, from a designer's perspective, one can explore countermeasures to secure the device at all operating frequencies while minimizing the design overhead. Thus a frequency-dependent noise-injection based compensation technique is proposed to efficiently protect against SCA. Correlation power analysis of AES (Advanced Encryption Standard) is carried at out at different frequency to observe the frequency dependency of SCA. The noise is injected and varied by using LFSRs and controlling the number of LFSRs in the circuit. It is observed that the implementations containing noise injector circuit require more traces to leak the key than those containing no such circuits.

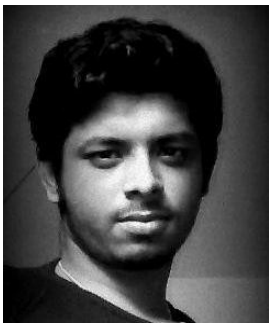
**Debasmita Lohar**
Email: debasmita.lohar@cse.iitkgp.ernet.in, dlohar2009@gmail.com
Joined the department in: December 2013

***Debasmita Lohar*** *received a B.Tech. Degree in Computer Science and Engineering from Heritage Institute of Technology, Kolkata, in 2013. From September 2013, she is working as a Research Consultant in the Department of Computer Science & Engineering, IIT Kharagpur, under the project: "Architectural and Algorithmic Optimizations for Speech based Communication Interfaces on Mobile Devices". Her research interests are in the areas of Probabilistic Program Analysis, Abstract Interpretation, Embedded System and Software Fault Tolerance.*
***Supervisor: Prof. Soumyajit Dey***

## Probabilistic Program Analysis for Software Reliability

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

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



**Parnab Kumar Chanda**
Email: parnab.2007@gmail.com
Joined the department in: December 2011

***Parnab Kumar Chanda*** *received a B.E. degree in Information Technology from School of Information Technology (formerly IIIT-Kolkata), WBUT Kolkata in 2009. From Jan 2010 till July 2011, he worked in Infosys Technologies, Chennai, as a Software Engineer. Since January 2012, he has been a research scholar in the department of Computer Science & Engineering in IIT Kharagpur. His research interests are in the area of Information Retrieval.*

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

## Cross Language Information Access

Web documents are growing with multilingual content every day. Since different medias, in countries like India and Europe, share the information like news, blogs, cinema, etc in the regional languages of the people, it becomes essential for the users to access the information rich content present across languages. Thus the need for a Cross Lingual Information Access (CLIA) system grows faster. Such systems would be expected to assist the information needs of the different language speaking users who may issue queries in one language by enabling them to access the information written in other languages. At present, we are looking at such a cross lingual information access system that is specifically intended for retrieval of documents written in Indian languages pertaining to the tourism domain. The basic idea of the CLIA system is as follows: A user is expected to choose any one of the 9 selected Indian languages or English and fire a query written in the language of their choice seeking certain information related to the tourism domain. CLIA system retrieves top k documents pertaining to the given user query and presents the ranked list of documents sorted by their similarity scores. The overall structure of the system has two parts: offline components and online components.

Offline components include: a web crawler (fetches html documents from the world wide web), parser (removes the noisy content and extracted the filtered text content with meta tags), language identifier (identifies the language of the document), domain specific document classifier (a document classifier to check whether the given document belongs to tourism or health or others), language specific stemmers and stop word remover (both for specific Indian languages), and indexer (to create an inverted index of the parsed web documents, each having specified fields)

Online components include: GUI (to feed the user queries by choosing the language of the choice of users), query processing module (forms the expanded query from the user keywords with specified boost factors for the fields), searcher (uses the ranking strategy that computes the similarity between the query and documents), output presentation (snippet and results page generation with further navigational links)

The ranking of web documents will be the primary focus in the current work. At present, the focus is on identifying the underlying topic(s) of the extracted content of each web document and then modeling and applying the ranking function using this topic information as a feature with various similarity measures. The final ordering of documents would be based on the similarity scores computed by the defined ranking function that maps the document topics with the actual intent of the user query.

**Partha De**
Email: partha.de@cse.iitkgp.ernet.in
Joined the department in: July 2010

***Partha De*** *received a B.Tech. degree in Computer Science from West Bengal University of Technology, Kolkata in 2005, and Post-graduate Diploma in Information Technology (PGDIT) from Indian Institute of Technology, Kharagpur in 2007. From September 2007 to June 2008, he worked in Indian Institute Technology, Kharagpur, as a Program Facilitator. From July 2008 to October 2009, he has been working as a Junior Project Assistant in the India Chip Design program in IIT Kharagpur. His research interests are in the areas of High-level Synthesis and secure transistor level circuit design.*

***Supervisor: Prof. Chittaranjan Mandal***

## Structure Architecture Driven High-level Synthesis for Array Intensive Applications

High-level synthesis (HLS) is the process of generating register transfer level (RTL) designs from the behavioral descriptions. To deal with the increasing complexity of today's VLSI designs, the use of HLS tools is crucial. Over the last several years, various such HLS tools have evolved which produce elementary non-optimized data paths to more sophisticated one generating data paths optimized with area, wire length, time, power, etc. Some of the existing HLS tools emphasis on optimization of layout area/wire length of the output RTL without considering an organization of the final data path at the start of the HLS process. We believe a better organization of the datapath and an abstract view of it at the input to a HLS tool along with the input behavior should give us optimized RTL with respect to layout area as well as wire length. With this objective, a HLS tool named “SAST” (Structured Architecture Synthesis Tool) has been developed in our group. A *simple but predictable* architecture called *structure architecture (SA)* has been proposed and forced the SAST to execute the input behavior on that architecture. SAST takes a behavioral description written in C-like language along with the parameters of the SA and generates synthesizable RTL. The SA is organized as architectural blocks (A-blocks). Each A-block has a local functional unit, local storage. All the A-blocks in a design are interconnected by a number of global buses. So, the structure of the final architecture is fixed at the start of the synthesis but the final interconnection will be finalized during the synthesis procedure. The advantage of this architecture is that the user has the full control over the final architecture and design space can be explored by simply changing the architectural parameters for the same input behaviour. Also, this structure data paths avoid random interconnects between data path components. The objective of my work is to validate our claim by extensive experimentation's. For this purpose, the RTLs generated by SAST from various benchmark problems need to be synthesized further with industrial tools such as Synopsis DA (for logic synthesis) and SoC Encounter from Cadence (for physical design) to obtain the actual measure of the layout area and wire length of the chip.

Presently, SAST does not support the use of arrays. My next objective is to extend SAST implementation to support arrays via local and global memories. Arrays used primarily by operations mapped to an A-block can be local to that A-block, whereas arrays needed by multiple A-blocks can be made global to those A-blocks.

## Secure cryptographic processor design to counter side channel attack (differential power analysis)

Side channel attack is any attack based on the information gained from the physical implementation of the cryptographic system rather than by brute force or theoretical weakness in cryptographic algorithms. Timing information, power consumption electromagnetic leaks, fault injection or even sound can provide extra source of information which can be exploited to break the system. Differential power analysis is one of the methods of side channel attack. Differential power analysis involves in collecting many power traces and performing statistical analysis of the power variation with respect to changes in data values and poses a serious threat so the cryptographic devices.

My aim is to build side channel (differential power) resistant AES and other cryptographic processor. It's easy to implement cryptographic algorithms in the case of software. The problem of this way is that such algorithms are typically too slow for real-time applications, such as storage devices, embedded systems, network routers, etc. A solution will be to implement such cryptographic algorithms in hardware. In cryptographic processor implementation, a dedicated cryptographic block of the cryptographic processor permits fast execution of encryption, decryption, and key scheduling operations. To build this a side channel attack resistant digital cell library comprising basic gates (NAND, NOR, AND, OR, XOR), adder, multiplier, flip-flop have been designed which will be used as a basic building block of cryptographic processor. My next objective is to fabricate cryptographic processor using UMC 65nm technology and also examine the power characteristics.

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

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

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

## Hardware Based Attacks on Cryptographic and Network Devices

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

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

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

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

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

## Differential Fault Attack prevention on AES using Infection Technique

Fault attacks are one of the most popular Side Channel Attacks on AES due to their simplicity. The introduction of easier fault induction techniques have further added to their feasibility. The basic idea is to inject a single(or multiple) fault(s) in the intermediate state of the cipher and then deploy linear or differential analysis strategies to reduce the key search space. To thwart this kind of attacks, two possible prevention technique can be used, such as, *Fault Detection* and *Infective Countermeasure*. Several studies show that *Detection Countermeasures* are easier to bypass as well as leaks information about the faults during comparison operations. For the last couple of years, Infection techniques gains a significant attention due to its unique yet simple and efficient structure. Our principle focus is to design an elegant algorithm for this purpose. We also implement and test our design in hardware platform to ensure that our scheme is both hardware and performence (with respect to time complexity) efficient.

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

***Shiladitya Ghosh*** *received his B.Tech. in Computer Science and 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 Indian Institute of Technology Kharagpur as a research scholar in January, 2014. His broad area of research is Formal analysis and design.*

***Supervisors: Prof. Chittaranjan Mandal and Prof. Pallab Dasgupta***

## Formal Modelling and Validation of Railway Interlocking

In railway electronic interlocking system, the automatic signalling equipment is programmed with the configuration data derived manually from the yard layout. This step is prone to human errors and any error can be a severe threat to signalling safety. The yard-layout data and the configured system both need to be verified to satisfy the desired safety requirements. The verification proccess 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. Accordingly, the contributions in the thesis include, (a) validation of inputs comprising validation of yard-layout data against some spatial properties and validating the control table against the layout, (b) efficient modelling of the interlocking system using the different relays (by reducing number of states by imposing input constraints and removing redundant states),(c) generation of yard-specific properties for verification of the model. To capture the actual environment, a set of complex properties including properties involving timers is considered. Higher level safety properties such as no-collision and no-derailment are also verified over the system. Presently,, I am working on automated generation of control table for a yard based on the safety rules laid out by the railways, taking the yard layout as inputs.

**Souvik Kolay**
Email: souvik1809@gmail.com
Joined the department in: December 2011

***Souvik Kolay*** *received a B.Tech. degree in Information Technology from RCC Institute of Information Technology, Kolkata in 2011. Since July 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 Lightweight Cryptography*

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

## Lightweight Crypto-primitives on FPGAs

Historically, cryptographic schemes have only been used for military or administrative purposes where secret information was to be transferred from one person to another. But with the changing times, it has found its use in a variety of applications so as to influence the daily life of normal human beings. From financial transactions to communication through electronic mails, from biometrics to database management systems - encryption of data to prevent it from getting into unwanted hands has become an absolute necessity. Cryptography has also evolved with time to suit these needs. With the development of new attacks, newer encryption schemes resistant to those attacks have come up. Again with the arrival of the Advanced Encryption Standard (AES), the need for a block cipher which serves as a standard has been satisfied. AES, however, works better on software than on hardware. In fact, it was designed with efficient software implementation in mind. But with the advent of pervasive computing and hence, the increased use of various smart devices like RFID tags, smart cards, wireless sensor nodes, and PDAs, the need of cryptographic systems to ensure security for these devices has also escalated. This means that a cryptographic scheme which does well for these kinds of devices is required. Moreover, as these devices have constrained memory, computing power and battery supply, the design of crypto primitives suited for such systems becomes all the more challenging. This area of cryptography which deals with the design, analysis and implementation of cryptographic algorithms and crypto-primitives for devices with extremely constrained resources is formally termed as lightweight cryptography.

Designing this kind of cryptographic algorithms always require a trade-off between security, efficiency and resources. As lightweight ciphers are constrained by area, power, and cost, application specific design opportunities in ASIC and amenability to mass productions makes ASIC a popular choice for lightweight crypto-systems. But ASIC chips cannot be reconfigured or modified. On the other hand, Field-programmable gate array (FPGAs) can be reconfigured or upgraded after manufacture. Although ASICs are popular choice for lightweight cryptography, recent low cost FPGAs make them an alternative for battery powered devices (WSN). Low cost FPGAs seem ideal for the customer producing small amount of WSN or RFIDs. The reconfiguration feature of FPGAs, allowing in-house update of design, is suited for designing lightweight cipher on FPGAs.

We proposes a new bit permutation instruction, called PERMS to accelerate software cryptography. Though most of the modern processor provides AES-NI instruction in the ISA to accelerate the AES algorithm, but there are many other cryptographic algorithms, which are

considered as ‘standard’ in commonly used security protocols. Many of these algorithms use bit permutation operation, which is quite slow in typical byte oriented processor. Further, we have come up with a new bit permutation instruction, PERMS, which can be used to accelerate these algorithms. The underlying bit permutation algorithm is based on bit swapping and has been developed analogous to comparison based sorting techniques. The swapping steps are stored as control bits, which is further used to perform the bit permutation. The newly proposed instruction is then compared with existing bit permutation instructions found in literature. The comparison with respect to the ‘scalability to perform large permutation’, ‘area requirement to provide hardware support’ and ‘throughput per area’ are found to be very competitive among the existing bit-permutation instructions. The PERMS instruction can be easily added with any of the existing 64 bit ISA. Due to the flexibility of required number of control bits, PERMS instruction can be expressed in various instruction formats, according to the ISA, where it is going to be added. Further, PERMS hardware needs only 670 GE, so it can also be considered for resource constrained devices, like Personal Digital Assistance (PDAs).

In the next phase of the work, we put forward an idea of a new lightweight block cipher, Khudra targeting the increasingly popular platforms of FPGAs. In Khudra, a variant of the generalized Feistel structure is used for the outer structure and the ‘F-function’ inside the outer structure is computed recursively by using the similar structure. We have provided a detailed security analysis of Khudra against both the classical cryptanalysis and newly proposed attacks. The cryptanalysis shows that Khudra can be considered to be secure against these kinds of attacks. In the subsequent section, we have discussed the implementation aspects of Khudra on both ASICs and FPGAs. Two different implementation strategies have been adopted for the implementation on ASICs and FPGAs. The implementation result of Khudra shows that it not only requires less resources on FPGA but also provides good throughput and throughput/slice ratio. Further, the estimated area for the ASIC implementation is also found to be very competitive among the existing lightweight block ciphers for ASIC.

**Srinivas Virinchi**
Email: virinchimnm@gmail.com
Joined the department in: July 2012

***Srinivas Virinchi*** *received a B.E. degree in Computer Science from Atria Institute of Technology, Bangalore in 2011. Since July 2012, he has been doing his MS in the department of Computer Science & Engineering in IIT Kharagpur. His research interests are in the areas of Data Mining and its application to Social Networks.*

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

## Link Prediction In Social Networks

Link prediction problem can be formally defined as follows: Given a social network at time t, we seek to predict the set of edges that will be added to the network during the time interval t to a future time interval t'. Link prediction can be used to recommend friends in a social network, predict relations between certain groups which would not be directly observed and suggesting research collaborations between researchers working in related areas. These methods used for link prediction can be based on the number of paths , neighborhood property of the nodes and other higher level approaches involving supervised and unsupervised learning. Some of the basic simple approaches are: more the number of common neighbors between two nodes, higher is possibility of link formation between the nodes; more the number of paths between two nodes, higher is the possibility of link formation between the two nodes.

### References

[1] D. Liben and N. J. Kleinberg, “The link prediction problem for social networks,” International conference on information and knowledge management, pages 556–559 , 2003.

**Suvadeep Hajra**
Email: suvadeep.hajra@gmail.com
Joined the department in: July 2011

***Suvadeep Hajra*** *received a B.E. degree in Computer Science & Engineering from Jadavpur University, Kolkata in 2005. After receiving his B.E., he worked in Software Industries for some time. Since July 2011, he has been a research scholar in the department of Computer Science & Engineering in IIT Kharagpur. His current research interests are in the areas of Cryptography.*

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

## Optimization of Non-profiling Multivariate Differential Power Analysis

In 1996, Paul Kocher introduces a new kind of cryptanalysis technique known as side-channel analysis. Unlike black-box cryptanalysis which attempts to discover the secret key from the algorithmic weakness of a cipher, side-channel analysis targets a particular implementation of the cipher. These kinds of attacks gather information about the secret key from various side-channel sources like power consumption, electromagnetic radiation, timing delay of a cryptographic device. Since side-channel attacks can recover secret key of various modern Ciphers including DES, AES, and RSA in a very short span of time (usually within hours), they pose an enormous threat to the information secrecy of the modern age.

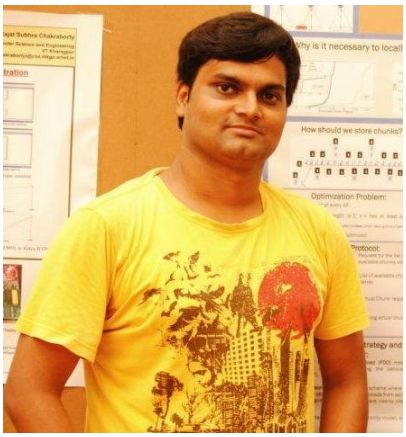
Power analysis attacks exploit the fact that power consumption of a hardware device depends on the operations as well as the data being processed within the device. Among those, Simple Power Analysis (SPA) attacks requires detail knowledge of the implementation to be successful. They can be easily prevented by various techniques like removal of conditional branches, addition of noise etc. The applicability of Power analysis has been vastly extended to a wide range by the introduction of Differential Power Analysis (DPA) which is based on data dependency of power consumption. Power consumption depends on the intermediate value processed on the device, the intermediate value again depends on the secret key, and thus the power consumption depends on the secret key used by the device. While based on this simple principle, DPA incorporates various statistical tools like difference-of-mean, correlation, and mutual information to make the attack useful in various adversarial conditions. These various adversarial conditions include the presence of electronic noise (caused by the inaccuracy of the measurement circuits, device behaviour etc.), algorithmic noise (introduced by the switching of bits which are not dependent upon the secret key), imperfection of the power consumption model (introduced due to the simplification of complex relation between the intermediate value processed by the device and the power consumption of the device). DPA uses power measurements of multiple encryption process along with the statistical tools to counteract the adversarial conditions. If the conditions are more adverse, more power measurements are needed to retrieve the correct key by an attack algorithm. On the other hand, lesser the number of required power measurements, stronger the attack algorithm. Since power measurements are the scarce resources, considerable efforts have been made to find new attack algorithms which are more powerful than the previous one.

In a real attack scenario, an intermediate variable (chosen such that it depends on a small part of the unknown key and the known plaintext/ciphertext) of the encryption algorithm is targeted. The attacker attempts to find the small part of the unknown key by exploiting the relation between the

targeted intermediate variable and the power consumption of the device at the time instant when the targeted intermediate variable is manipulated. This method is known as univariate DPA, since it exploits the leakage of only on time instant. Though univariate DPA is effective in most of the modern attack scenarios, its performance is limited by maximum Signal-to-Noise ratio (SNR) of the power measurements. This puts a serious challenge to the attacker in situations where SNR of the power measurements is very low.

In most of the modern measurement setup, a large number of power measurements are collected during the computation of the targeted intermediate variable. As a consequence, all the power measurements in a certain window contain some information about the targeted intermediate variable. This research proposes multivariate DPA as a way to increase the SNR of power measurements by combining the power consumptions of all the time instants in the predetermined window with help of a novel multivariate power consumption model. The novel multivariate power consumption model provides a natural platform to extend most of the existing univariate DPA to multivariate DPA, thus enables the attacker to overcome the limitation of univariate DPA.

Besides this, I am involved in a project which aims to design a DPA resistant block cipher. For this purpose, we have chosen tweakable block cipher where, beside the plaintext and the secret key, the ciphertext depends on a third input called tweak. The tweak input is kept secret. The unknown tweak obfuscates the relation between the secret key and the intermediate value. On the downside, encryption and decryption operations must be synchronized with the same tweak. We have been able to show that this scheme is provably secure against DPA.



**Swadhin Pradhan**
Email: swadhin.pradhan@cse.iitkgp.ernet.in, swadhinjeet88@gmail.com
Joined the department in: July 2012

***Swadhin Pradhan*** *received his B.E. degree in Information Technology from Jadavpur University in 2011. From May 2011 till February 2012, he worked in Interra Systems India Pvt. Ltd., Kolkata, as a Software Engineer. Since July 2012, he has been pursuing his MS (by research) in Department of Computer Science & Engineering Department, IIT Kharagpur. His research interests are in the areas of Mobile Systems & Wireless Internet.*

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

## Identifying Invisible Natural Landmarks using Smart phones

Today's smart phones are equipped with numerous sensors, e.g., gyroscope, magnetometer, accelerometer etc. which can tap into the surroundings. This sensory information from the surroundings gives different cues which are beyond the perception of human beings. Our key observation is that certain locations in both indoor and outdoor environment, present identifiable signatures on one or more sensing dimensions. An elevator, for instance, imposes a distinct pattern on a smart phone's accelerometer; a corridor-corner may overhear a unique set of Wi-Fi access points; a specific spot may experience an unusual magnetic fluctuation. We hypothesize that these kinds of signatures naturally exist in the environment, and can be envisioned as landmarks of a place. However, enumerating these natural landmarks is not trivial. Energy constraints, device heterogeneities, human mobility diversity, frequent environmental changes etc. can pose difficulties in landmark generation and stability of landmarks across different parameters. To find out the difficulties in this scheme, we have developed an android application and employed a small scale experiment in our department to enumerate the landmarks. Moreover, we are developing a lightweight unsupervised scheme to generate landmarks from raw sensor data and also looking into the different factors of creation and stability of landmarks. We envision that the future indoor and outdoor maps will be annotated with these types of smart phone sensors' based landmarks which will help in augmented reality applications and location based services. To support this claim, we have built a retail analytics cum shopping android application, *RetailGuide*, for super markets using these smartphone based stable landmarks.

## Aggregating Inter-App Traffic to reduce Energy Consumption in Smartphones

Surging popularity of network centric apps for smartphones is driven by cloud computing. Many of these apps run as background services, waking up intermittently to synchronize with the servers. This triggers frequent small sized request packets that activate the radio interface. It has been noted that frequent card activation wastes battery due to high switching energy. Hence the challenge is to maximize the radio resource utilization on each card activation. Two factors contribute to low utilization. First, apps are not synchronized to wake up simultaneously. Second, high speed cellular access links push the bottleneck to the network core leading to low bandwidth utilization of the access

link. In this work, we address the challenges by improving radio usage through delayed batched scheduling of packets across apps. This also increases bandwidth utilization by interleaving request response packets from different apps without incurring switching cost. We propose three online techniques that reduce network energy usage. A variable delay budget is assigned to each background app based on user's interaction with the app. Foreground apps are always prioritized to minimally impact user experience. Using app usage models, we simulate the overall traffic from a smartphone. Synthetic traffic traces representing different foreground app usage, such as gaming, browsing, and streaming, in presence of background services, are generated. The trace driven simulation results show that online batch scheduling can achieve 40% energy savings, computed using the standard 3G radio energy model.

# 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 Assistant Professor in the Department of Computer Science and Engineering, Indian Institute of Technology Kharagpur. Prior to this, he worked as 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

**Anupam Basu**
Email: anupam@cse.iitkgp.ernet.in

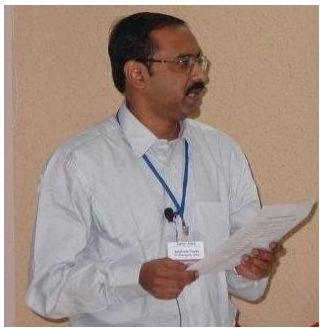
***Research Interests:*** *Emdedded systems, cognitive science and language processing with particular focus on intelligent interface design and human computer interaction*

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.

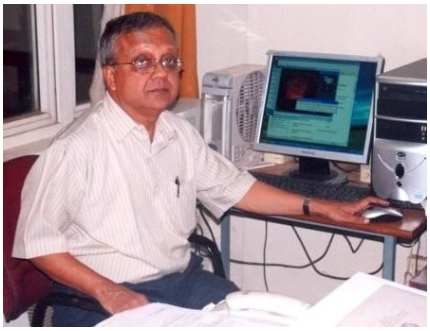
He has won several awards and honors for his research contributions. These include the National Award for the Best Technology Innovation for the Physically Disabled (2007), the Da Vinci Award 2004, and Outstanding Young Person Award 1996.



**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 and School of IT. 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*

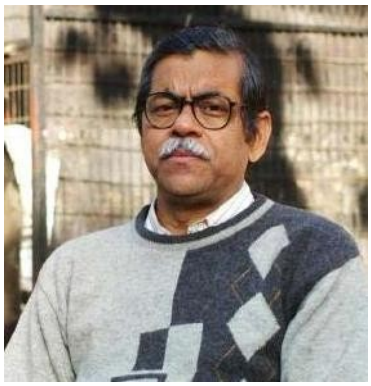
Chittaranjan Mandal received his Ph.D. degree from IIT, Kharagpur, India, in 1997. He is currently a Professor with the Department of Computer Science and Engineering and also the School of Information Technology, IIT, Kharagpur. Earlier he served as a Reader with Jadavpur University. His research interests 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.

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

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

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

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



**Dipankar Sarkar**
Email: ds@cse.iitkgp.ernet.in

***Research interests:*** *Formal verification and symbolic reasoning*

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

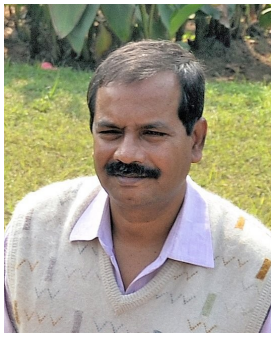
**Goutam Biswas**
Email: goutam@cse.iitkgp.ernet.in

***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).

**Niloy Ganguly**
Email: niloy@cse.iitkgp.ernet.in

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

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

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

**Pabitra Mitra**
Email: pabitra@cse.iitkgp.ernet.in

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

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

**Pallab Dasgupta**
Email: pallab@cse.iitkgp.ernet.in

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

Dr. Pallab Dasgupta did his B.Tech, M.Tech and PhD in Computer Science from the Indian Institute of Technology Kharagpur. He is currently a Professor at the Dept. of Computer Sc. & Engg, I.I.T. Kharagpur. His research interests include Formal Verification, Artificial Intelligence and VLSI. He has over 100 research papers and 2 books in these areas. He currently leads the Formal Verification group at the CSE Dept, IIT Kharagpur

http://www.facweb.iitkgp.ernet.in/~pallab/forverif.html

which has been developing validation technology for several companies, including Intel, Synopsys, General Motors, SRC and National Semiconductors. Since Oct 2007, he is also the Professor-in-charge of the Advanced VLSI Design Lab, IIT Kharagpur. Dr Dasgupta has been a recipient of the Young Scientist awards from the Indian National Science Academy, Indian National Academy of Engineering, and the Indian Academy of Science. He is a senior member of IEEE.

Dr. Dasgupta is currently holding the position of Associate Dean of Sponsored Research and Industrial Consultancy (SRIC).

**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, 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 General Chair for International Conference on VLSI Design & Embedded Systems in 2005 and in various capacities for International Symposium on VLSI Design & Test in 2007, 2008 and 2012. He is currently the Editor-in-Chief of The Journal of Institution of Engineers: Series B, reviewer for Pattern Recognition Letters and a Review Writer for ACM Computing 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), 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), Indian Unit for Pattern Recognition and Artificial Intelligence (IUPRAI) and VLSI Society of India (VSI).

**Partha Sarathi Dey**

Email: psd@cse.iitkgp.ernet.in

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

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

**Pawan Goyal**

Email: pawang@cse.iitkgp.ernet.in

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

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

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

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

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

***Research Interests:*** *Computational biology and bioinformatics*

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

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

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

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

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

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

**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.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

# Publications by Research Scholars (2013 – 2014)

**Journal papers**

1. Bhattacharyya, S., A. Biswas, J. Mukherjee, A. K. Majumdar, B. Majumdar, S. Mukherjee, A. K. Singh, Detection of artifacts from high energy bursts in neonatal EEG, *Computers in Biology and Medicine*, Volume 43, Number 11, 1804–1814, 2013.

2. Chakraborty, R. S., I. Saha, A. Palchaudhuri and G. K. Naik, Hardware Trojan Insertion by Direct Modification of FPGA Configuration Bitstream, *IEEE Design and Test of Computers*, vol. 30, No. 2, 45–54, 2013.

3. Chakraborty, T., S. Srinivasan, N. Ganguly, S. Bhowmick and A. Mukherjee, Constant Communities in Complex Networks, *Nature Scientific Reports* 3, 2013.

4. Hazra, A., P. Ghosh, S. G. Vadlamudi, P. P. Chakrabarti and P. Dasgupta, Formal Methods for Early Analysis of Functional Reliability in Component-Based Embedded Applications, *IEEE Embedded Systems Letters* (*ESL*), Volume 5, Issue 1, 8–11, 2013.

5. Hazra, A., S. Goyal, P. Dasgupta and A. Pal, Formal Verification of Architectural Power Intent, *IEEE Transactions on Very Large Scale Integration Systems* (*TVLSI*), Volume 21, Issue 3, 78–91, 2013.

6. Hazra, A., R. Mukherjee, P. Dasgupta, A. Pal, K. Harer, A. Banerjee and S. Mukherjee, POWER-TRUCTOR: An Integrated Tool Flow for Formal Verification and Coverage of Architectural Power Intent, *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems* (*TCAD*), Volume 32, Issue 11, 1801–1813, 2013.

7. Karfa, C., K. Banerjee, D. Sarkar and C. Mandal, Verification of Loop and Arithmetic Transformations of Array-Intensive Behaviours, *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems* (*TCAD*), Volume 32, Nov 2013, 1787–1800, 2013.

8. Maity, S. K., A. Mukherjee, F. Tria and V. Loreto, Emergence of fast agreement in an overhearing population: The case of the naming game, *Europhysics Letters* (*EPL*), Volume 101, Number 6, 2013.

9. Mallick, T., P. P. Das and A. K. Majumdar, Characterizations of Noise in Kinect Depth Images, *IEEE Sensor Journal*, to appear, 2014.

10. Mazumdar, B., D. Mukhopadhyay and I. Sengupta, Constrained Search for a Class of Good Bijective S-Boxes with Improved DPA Resistivity, *IEEE Transactions on Information Forensics and Security*, Volume: 8, Issue: 12, 2154–2163, 2013.

11. Mishra, T. K., S. P. Pal, Lower Bounds for Ramsey Numbers for Complete Bipartite and 3-Uniform Tripartite Subgraphs, *Journal of Graph Algorithms and Applications*, Volume 17, Issue 6, 671–688, 2013.

12. Pratihar, S., P. Bhowmick, S. Sural and J. Mukhopadhyay, Skew Correction of Document Images by Rank Analysis in Farey Sequence, *International Journal of Pattern Recognition and Artificial Intelligence*, Vol. 27(7), 35 pages, 2013.

13. Saha, S., R. Kumar, G. Baboo, Characterization of graph properties for improved Pareto fronts using heuristics and EA for bi-objective graph coloring problem, *Applied Soft Computing*, 13(5), 2812–2822, 2013.

14. Santosh Prabhu M., A. Hazra and P. Dasgupta, Reliability Guarantees in Automata Based Scheduling for Embedded Control Software, *IEEE Embedded Systems Letters* (*ESL*), Volume 5, Issue 2, 17–20, 2013.

**Conference papers**

1. Basu Roy, D., D. Mukhopadhyay, M. Izumi, J. Takahashi, Tile before Multiplication: An efficient strategy to optimize DSP multiplier for Accelerating Prime Field ECC for NIST Curves, *DAC-2014*, 2014.

2. Bhattacharya, P., 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.

3. Bhattacharyya, S., A. Biswas, R. Pandit, J. Mukherjee, A. K. Majumdar, B. Majumdar, S. Mukherjee, and A. K. Singh, Detection of Burst-Suppression in Neonatal EEG, *International Conference on VLSI and Signal Processing* (*ICVSP*), 2014.

4. Chakraborty, T. and A. Chakraborty, OverCite: Finding Overlapping Communities in Citation Network, In *Proceedings of IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining* (*ASONAM*), 1124–1131, 2013.

5. Chakraborty, T., N. Ganguly and A. Mukherjee, Rising Popularity of Interdisciplinary Research – an Analysis of Citation Networks, *Workshop on Science and Engineering of Social Networks* (*SCINSE*), *6th International Conference on Communication System and Networks* (*COMSNETS-2014*), 2014.

6. Chakraborty, T., S. Kumar, M D. Reddy, S. Kumar, N. Ganguly and A. Mukherjee, Automatic Classification and Analysis of Interdisciplinary Fields in Computer Sciences, *2013 ASE/IEEE International Conference on Social Computing* (*SocialCom-2013*), 180–187, 2013.

7. Chakraborty, T., S. Sikdar, V. Tammana, N. Ganguly and A. Mukherjee, Computer Science Fields as Ground-truth Communities: Their Impact, Rise and Fall, *IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining* (*ASONAM*), 426–433, 2013.

8. Dandapat, S. K., S. Pradhan, and N. Ganguly, Offloading Cellular Network, *IBM ICARE*, 2013.

9. Dandapat, S. K., S. Pradhan, R. Roychoudhury, and N. Ganguly, Sprinkler: Distributed content storage for just-in-time streaming, *ACM CellNet MobiSys workshop*, 2013.

10. Das, A. and S. Sarkar, Word Sense Disambiguation in Bengali applied to Bengali-Hindi Machine Translation, *International Conference on Natural Language Processing*, Volume 10, Issue 1, 20–29, 2013.

11. De, P., K. Banerjee, C. Mandal and D. Mukhopadhyay, Designing DPA Resistant Circuits Using BDD Architecture and Bottom Pre-charge Logic, *Euromicro Conference on Digital System Design* (*DSD*), 641–644, 2013.

12. Dhal, S. and I. Sen Gupta, A New Authentication Protocol for RFID communication in Multi-tag Arrangement, *International Conference on Computing for Sustainable Global Development INDIACom*, to appear, 2014.

13. Dhal, S. and I. Sen Gupta, Protocol to Authenticate the Objects Attached with Multiple RFID tags, *Emerging Trends in Computing and Communication ETCC*, to appear, 2014.

14. Ghosh, S., M. B. Zafar, P. Bhattacharya, N. Sharma, N. Ganguly, and K. P. Gummadi, On Sampling the Wisdom of Crowds: Random vs. Expert Sampling of the Twitter Stream, *ACM Conference on Information and Knowledge Management* (*i*), Burlingame, CA, USA, 2013.

15. Ghoshal, B. and I. Sen Gupta, A Distributed BIST Scheme for NoC-Based Memory Cores, *Euromicro Conference on Digital System Design* (*DSD 2013*), 567–574, 2013.

16. Ghoshal, B., C. Mandal and I. Sengupta, Re-using Refresh for Self-testing DRAMs, *International Symposium on Eletronic System Design* (*ISED 2013*), 2013.

17. Hajra, S. and D. Mukhopadhyay, Multivariate Leakage Model for Improving Non-profiling DPA on Noisy Power Traces, *INSCRYPT*, 1–18, 2013.

18. Hajra, S. and D. Mukhopadhyay, On the Optimum Pre-processing for Non-profiling DPA, *COSADE*, to appear, 2014.

19. Hajra, S., C. Rebeiro, S. Bhasin, G. Bajaj, S. Sharma, S. Guilley and D. Mukhopadhyay, DRECON: DPA Resistant Encryption by Construction, *AFRICACRYPT*, to appear, 2014.

20. Karfa, C., K. Banerjee, D. Sarkar and C. Mandal, Experimentation with SMT Solvers and Theorem Provers for Verification of Loop and Arithmetic Transformations, *IBM Collaborative Academia Research Exchange* (*I-CARE*), 3:1–3:4, 2013.

21. Karmakar, S. and D. Roy Chowdhury, Leakage Squeezing using Cellular Automata, *Automata 2013*, 98–109, 2013.

22. Karmakar, S. and D. Roy Chowdhury, Differential Fault Analysis of MICKEY-128 2.0, *IEEE FDTC 2013*, 52–59, 2013.

23. Khurana, S., S. Kolay, C. Rebeiro and D. Mukhopadhyay, Lightweight Cipher Implementations on Embedded Processors, *Design & Technology of Integrated Systems in Nanoscale Era* (*DTIS*), IEEE, 82–87, 2013.

24. Kolay, S., S. Khurana, A. Sadhukhan, C. Rebeiro and D. Mukhopadhyay, PERMS: A Bit Permutation Instruction for Accelerating Software Cryptography, E*uromicro Conference on Digital System Design* (*DSD*), IEEE, 963–968, 2013.

25. Kuila, S., D. Saha, M. Pal and D. Roy Chowdhury, Practical Distinguishers Against 6-Round Keccak-f Permutation Exploiting Self-Symmetry, *7th International Conference on Cryptology in Africa* (*Africacrypt 2014*), to appear, Morocco, 2014.

26. Maity, S. K. and A. Mukherjee, Understanding how learning affects agreement process in social networks, *IEEE/ASE International Conference on Social Computing*, 2013.

27. Mallick, T., P. P. Das and A. K. Majumdar, Study of Interference Noise in Multi-Kinect Set-up, *International Conference on Computer Vision Theory and Applications* (*VISAPP 2014*), 173–178, 2014.

28. Mallick, T., P. P. Das and A. K. Majumdar, Estimation of the orientation and distance of a mirror from Kinect depth data, National *Conference on Computer Vision, Pattern Recognition, Image Processing and Graphics* (*NCVPRIPG 2013*), 2013.

29. Mazumdar, B., D. Mukhopadhyay, and I. Sengupta, Design and Implementation of Rotation Symmetric S-boxes with High Nonlinearity and High DPA Resilience, *6th IEEE International Symposium on Hardware Oriented Security and Trust* (*HOST*), 2013.

30. Mishra, T. K., S. P. Pal, Lower Bounds for Ramsey Numbers for Complete Bipartite and 3-Uniform Tripartite Subgraphs, *WALCOM: Algorithms and Computation*, LNCS 7748, 257–264, 2013.

31. Mukherjee, J. C. and A. Gupta, A mobility aware scheduler for low cost charging of electric vehicles in smart grid, *Sixth International Conference on Communication Systems and Networks* (*COMSNETS*), 1–8, 2014.

32. Mukherjee, J. C. and A. Gupta, Mobility Aware Charge Scheduling of Electric Vehicles for Imbalance Reduction in Smart Grid, *Fifteenth International Conference on Distributed Computing and Networking* (*ICDCN*), 378–392, 2014.

33. Pradhan, S., A. Balashankar, N. Ganguly and B. Mitra, (Stable) Virtual Landmarks: Spatial Dropbox to enhance Retail Experience, *COMSNETS 2014*, 2014.

34. Pratihar, S., P. Bhowmick, S. Sural, and J. Mukhopadhyay, Removal of Hand-drawn Annotation Lines from Document Images by Digital-geometric Analysis and Inpainting, *NCVPRIPG 2013*, 2013.

35. Pyne, S. and A. Pal, Energy Efficient Array Initialization Using Loop Unrolling with Partial Gray Code Sequence, *17th International Symposium on VLSI Design and Test* (*VDAT 2013*), Jaipur, India, CCIS, Springer, Volume 382, 83–93, 2013.

36. Raha, R., S. Dey, P. P. Chakrabarti, P. Dasgupta, Multi-mode Sampling Period Selection for Embedded Real-Time Control, *Design Automation Conference* (*DAC*), to appear, accepted as poster presentation, 2014.

37. Ramanath, R., M. Choudhury, K. Bali and R. Saha Roy, Crowd Prefers the Middle Path: A New IAA Metric for Crowdsourcing Reveals Turker Biases in Query Segmentation, *51st Annual Meeting of the Association for Computational Linguistics* (*ACL '13*), 1713–1722, 2013.

38. Saha Roy, R., A. Suresh, N. Ganguly and M. Choudhury, Place Value: Word Position Shifts Vital to Search Dynamics, *22nd International World Wide Web Conference 2013* (*WWW '13*), 153–154, 2013.

39. Saha Roy, R., M. Choudhury, P. Majumder and K. Agarwal, Overview and Datasets of FIRE 2013 Track on Transliterated Search, *Fifth Forum for Information Retrieval Evaluation 2013* (*FIRE '13*), 2013.

40. Saha Roy, R., M. Dastagiri Reddy, N. Ganguly and M. Choudhury, Understanding the Linguistic Structure and Evolution of Web Search Queries, *10th International Conference on the Evolution of Language* (*Evolang X*), 14–17, 2014.

41. Saha Roy, R., N. Ganguly and M. Choudhury, Structural Complexity of Web Search Queries through the Lenses of Positionality, Language Models and Networks, *10th European Conference on Complex Systems* (*ECCS '13*), 75, 2013.

42. Sahoo, D. P., D. Mukhopadhyay and R. S. Chakraborty, Design of Low Area-overhead Ring Oscillator PUF with Large Challenge Space, *International Conference on Reconfigurable Computing and FPGAs* (*ReConFig*), Cancun, Mexico, 2013.

43. Sahoo, D. P., D. Mukhopadhyay and R. S. Chakraborty, Formal Design of Composite Physically Unclonable Function, *Security Proofs for Embedded Systems* (*PROOFS*), Santa Barbara, California, USA, 2013.

44. Santosh Prabhu M., A. Hazra, P. Dasgupta and P. P. Chakrabarti, Handling Fault Detection Latencies in Automata-based Scheduling for Embedded Control Software, *IEEE Multi-Conference on Systems and Control* (*MSC*), 1–6, 2013.

45. Sengupta, B. and A. Das, SIMD-Based Implementation of Sieving in Integer-Factoring Algorithms, *3rd International Conference on Security, Privacy, and Applied Cryptography Engineering* (*SPACE '13*), 2013.

46. Singh, A. K. and S. Dhal, I. Sen Gupta, An Approach to Solve Tracking and Message Blocking Problems in RFID, *International Conference on Communications System and Network Technology* (*CSNT*), to appear, 2014.

47. Sinha, P., A. Dutta Choudhury, A. K. Agarwal, Sentiment Analysis of Wimbledon Tweets, *ACM WWW 2014 Microposts Workshop*, 2014.

48. Srinivas V. and P. Mitra, Similarity Measures for Link Prediction Using Power Law Degree Distribution., *ICONIP*, LNCS 8227, 257–264, 2013.

49. Srinivas V. and P. Mitra, Link Prediction Using Power Law Clique Distribution and Common Edges., *PREMI*, LNCS 8251, 739–744, 2013.

50. Wang, X., W. Yueh, D. Basu Roy, S. Mukhopadhyay, D. Mukhopadhyay and S. Bhunia, Role of Power Grid in Side Channel Attack and Power-Grid-Aware Secure Design, *DAC*, article no. 78, 2013.

# Awards and Achievements by Research Scholars (2013 – 2014)

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

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

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

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

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

# Research Scholars Who Graduated in 2013 – 2014

## PhD Students

1. **Chhabi Rani Panigrahi**
2. **Priyankar Ghosh**
3. **Srobona Mitra**
4. **Saptarshi Ghosh**
5. **Sk. Subidh Ali**
6. **Dinesh Das**
7. **Soumen Bag**
8. **Pravanjan Choudhury**

## MS Students

1. **Ritwika Ghose**
2. **Debmalya Sinha**
3. **Sandipan Mandal**
4. **Rajdeep Mukherjee**
5. **Sirsendu Mohanta**
6. **Biswanath Barik**
7. **Chandan Misra**
8. **Satrajit Ghosh**


INDIA INSTITUTE OF TECHNOLOGY