Research Scholars' Day 2013

Department of Computer Science & 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.

Like the previous year, this year also we are holding our research scholar day on the 23rd March, 2013. This is the fourth occasion when we, all, will assemble together and get a glimpse of our current research activities from our students. No doubt this year too the day will be observed with equal enthusiasm and zeal by our PhD and MS students, who would take this opportunity to demonstrate their latest research findings and to exchange ideas of research, development, and knowledge among the different research groups and faculties of the department. My best wishes are with them in this endeavor.

Jayanta Mukhopadhyay

PhD & MS SCHOLARS

List of PhD Students

Kallol Mallick
Srobona Mitra
Priyankar Ghosh
Rajiv Ranjan Suman
Sanjay Chatterji
Mounendra Sankar Desarkar
Sk. Subidh Ali
Rajendra Prasath R
Prasenjit Mondal
Soumyadip Bandyopadhyay
Ishani Chakraborty
Bodhisatwa Mazumdar
Saptarshi Ghosh
Rajib Ranjan Maiti
Manjira Sinha
Chhabi Rani Panigrahi
Soma Saha
Sourav Kumar Dandapat
Kamalesh Ghosh
Rebeiro Chester Dominic
Satya Gautam Vadlamudi
Sudip Roy
Rishiraj Saha Roy
Sumanta Pyne
Bibhas Ghosal
Subhasish Dhal
Kunal Banerjee
Tirthankar Dasgupta
Aritra Hazra
Subhadip Kundu
Paranatapa Bhattacharya
Ruchira Naskar
Sabyasachi Karati
Mahesh Raghunath Shirole
Sudipta Saha
Partha Sarathi Dey
Sandip Karmakar
Srimanta Kundu
Joy Chanadra Mukherjee
Tripti Swarnkar
Sanjoy Pratihar
Tanmoy Chakraborty
Anupam Mandal
Tanwi Mallick
Durga Prasad Sahoo
Abir De
Sourya Bhattacharyya
Prajna Devi Upadhyay
Jimmy Jose
Dhiman Saha
Ranita Biswas
Priyanka Sinha
Moumita Saha
Anju P.J.
Sumana Ghosh
Sandipan Sikdar

List of MS Students

Biswanath Barik
Praloy Kr. Biswas
Sirsendu Mohanta
Sandipan Mandal
Ritwika Ghose
Prasenjit Dhole
Debmalya Sinha
Biswanath Saha
Rajdeep Mukherjee
Binanda Sengupta
Partha De
Tamal Sen
Suman Kalyan Maity
Suvadeep Hajra
Indrasish Saha
Pranab Kr. Chanda
Ayan Palchaudhuri
Arnab Dhar
Souvik Kolay
Debapriya Basu Roy
Srinivas Virinchi
Swadhin Pradhan
Shamit Ghosh
Abhrajit Sengupta

Research Abstracts of PhD and MS Scholars

PhD Scholars

Sanjay Chatterji

Email: schatt@cse.iitkgp.ernet.in
Joined the department in: January 2008

Sanjay Chatterji *earned Bachelor in Technology degree from Computer Science and Engineering of Haldia Institute of Technology in 2003 and Master of Engineering degree from Computer Science and Technology of Bengal Engineering and Science University (Formerly B.E. College), Shibpur in 2005. He worked as a lecturer in CSE Department of HIT, Haldia for 1 year and in CSE Department of KNSIT, Bangalore for 1 year. Since January 2008, he has been a research scholar in the department of Computer Science and Engineering of IIT Kharagpur. His research interests are in the areas of Computational Linguistics, Natural Language Processing and Machine Translation.*

Supervisors: Prof. Sudeshna Sarkar and Prof. Anupam Basu

Hybrid Approaches to Bengali Hindi Machine Translation

Machine Translation: Machine translation is the application of computers to the task of translating texts from one natural language to another. It gives a word sequence of target language for a given source language word sequence. In this process the meaning of the source language text must be preserved in the generated text in the target language. The translation process may be stated as decoding the meaning of the source text and re-encoding this meaning in the target language. There are mainly two ways of performing the machine translation - rule based machine translation (RBMT) and statistical machine translation (SMT). RBMT relies on built-in linguistic rules and resources. Developing a RBMT involves a great deal of time and linguistic expertise. SMT on the other hand provides good quality translation when large and good quality parallel corpus is available. It creates statistical model from the parallel corpus. But when parallel corpus are not available or are only available in limited quantities, one may go for a combined approach making use of simple rules and supplemented by small parallel corpora. Recent works on SMT have led to significant progress in coverage and quality of the translation systems but the amount of work involving translation into Indian languages, like Bengali or Hindi, is quite limited.

Hybrid1: We have attempted to combine different types of knowledge and developed a hybrid

system for the Bengali-Hindi language pair. The overall translation quality is improved by exploiting explicit linguistic knowledge contained in the rules and resources of the RBMT system and implicit knowledge that can be extracted from the SMT system. We have used language resources such as dictionary, suffix list, rules etc. to improve the SMT output quality. The open source decoder called Moses is used to get the baseline translation with the help of a parallel corpus of 12,000 sentences. We have used a modification of BLEU score methodology to consider concepts rather than words in evaluation process. We have restricted our experiments for Bengali to Hindi machine translation. We have crawled a 500K word corpora of Bengali and Hindi languages each. Using these resources and developing the rules we have developed one Bengali to Hindi Hybrid Machine Translation System.

Hybrid2: Recently some work has been done on a transfer based Bengali to Hindi machine translation system. A Bengali to Hindi transfer based baseline machine translation system is developed in the ILMT project sponsored by MCIT, Govt. of India. The baseline system replaces Bengali word with the most frequent Hindi word. But, the most frequent translation may not be the proper translation for a specific context. We have used a method to find the better lexical choice among the dictionary options with the help of the contextual information of a Hindi monolingual corpus. This approach takes Bengali sentence and converts it to Hindi sentence with the help of lattice-based data structure. The baseline and proposed translation systems are evaluated using the BLEU automatic metric and human evaluation process and later system is found performing better in both evaluations.

Noise Correction: Output of machine translation system needs to be corrected to get a meaningful target sentence. Our approach to correcting noise in the sentences consists of correcting noise in the phrases of the sentence. For this, we split the sentence into small phrases. We use the n-gram language model obtained from a monolingual corpus. Given a short phrase from the noisy sentence, we search for the short phrases in the language model which are frequent and similar to the noisy sentence phrase. These searched phrases are candidates of the noisy sentence phrase. For finding suitable candidate phrases for each short phrase of noisy sentence, it does not suffice to only search for the frequent exact phrases in the language model which are similar to the input phrase. We search other variations of the words of this short phrase, e.g., spelling variation, morphological variation and lexical variations for retrieval.

Maunendra Sankar Desarkar
Email: maunendra@cse.iitkgp.ernet.in
Joined the department in: July 2008

Maunendra Sankar Desarkar *received a B.E. degree in Computer Science from the University of Burdwan in 2004 and an M.Tech. degree in Computer Science from Indian Institute of Technology Kanpur in 2006. From July 2006 till July 2008, he worked in Sybase India Pvt. Ltd as a Software Developer. Since July 2008, he has been a research scholar in the department of Computer Science & Engineering in IIT Kharagpur. He received the Microsoft Research India PhD fellowship from Microsoft Research India in 2009. His research has won several awards and accolades such as Honorable Mention Award in Yahoo Key Scientific Challenge 2012 and best research presentation in IDRBT doctoral colloquium 2012. His research interests are in the areas of Recommender Systems, Data Mining and Information Retrieval.*

Supervisor: Prof. Sudeshna Sarkar

Algorithms for Personalized Recommender Systems

Recommender systems suggest or recommend different items or services to the users. The item types range from movie DVDs, music CDs, books to scientific papers, news articles, video clips to even complex sets like travel packages, and links in social networks. We look at few aspects that the recommender systems need to focus on for generating effective recommendations. For example, recommendations generated by a system for a particular user are generally personalized to the taste of the user. Hence, the system should understand the taste or the interest profile of the user. In order to get this information, the systems rely on the feedbacks received from the users. Determining the type of feedback to be used is one important aspect of recommender system design. We have used relative preference information as user feedback. Temporal information is another important aspect. Changes in users' interest profile (user dynamics) and the items' selling trends (item dynamics) are some important features that should be given importance to. We have based our research on Recommender Systems on these two aspects.

Several recommender systems allow users to express their opinions about different items by rating them on a fixed rating scale. The rating assigned by a user to an item may be treated as the utility of the item for the user. If the system can predict the (personalized) utilities of different

items for a user, then that information can be used for recommending items to that user. This argument has given rise to the *rating prediction problem* in recommender systems where the task is to predict the rating that a user would give to an item that he/she has not rated in the past.

Neighborhood based collaborative filtering is a widely used framework for rating prediction in recommender systems. Based on the assumption that users with similar tastes would rate items similarly, this framework first finds a group of users having similar interests. Ratings given by the users from that group are used to predict unknown ratings. User-based collaborative filtering algorithms assign weights to the users to capture similarities between them. The weighted average of similar users' ratings for the test item is output as prediction.

We developed a *preference relation based collaborative filtering algorithm* for the Rating Prediction problem. Collaborative systems looking at ratings only have some drawbacks. Users have different levels of leniency while rating items. So even similar users tend to rate the same items differently. Moreover, it might be difficult to pick a particular rating for an item, whereas given two different items it is probably easier to say which one is better (or both are equally good). Some other problems are related to the inconsistency of ratings, choice limitation due to the rating scale etc. We believe that the use of preference relations can eliminate/reduce some of these problems. We propose a collaborative filtering approach that uses preference relations between items instead of absolute ratings. The approach views each user's ratings as a preference graph. Similarity weights are learned using an iterative method motivated by online learning. These weights are used to create an aggregate preference graph. Ratings are inferred to maximally agree with this aggregate graph. Empirical results show that our method outperforms other methods in the sparse regions.

We have also incorporated *preference relations in the matrix factorization framework*. From the absolute ratings provided by the users, we induce preference relations and input those to the proposed algorithm. The algorithm models each user and each item as a point in a low dimensional feature space. Each dimension can be viewed as a hidden category mined from the data. The low dimensional feature representation of an item suggests the item’s belongingness to those latent categories. The feature representation of a user suggests the user’s affinities to those categories. The system may use these feature representations to predict the items’ utilities to the users. We have used this technique for both rating prediction and item recommendation tasks. Experimental results on benchmark dataset show the efficacy of the proposed algorithms.

We also study recommender algorithms that consider *temporal information for item recommendation*. We look at ways of incorporating purchase time information in the standard user based collaborative filtering algorithms. Users’ interests may shift over time. Recommender systems should therefore rely on recent purchases of the users. Items also have their own dynamics. Most of the items in a recommender system are widely popular just after their releases but do not sell that well afterwards. The proposed algorithms use the time-of-purchase information for calculating user similarities. The time information is also used while combining the *purchase behaviors* of the *experts* and generating the final recommendation. Experimental comparisons performed on several benchmark datasets indicate that the recommendation performance can be improved by considering the recent purchases of the users and the experts.

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.*

Supervisor: 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. on. We have developed a unified approach to handle all these effectively. This approach consisting of indexing several variations of each input phrase, and considering these variations for retrieval.

Sudip Roy
Email: sudipr@cse.iitkgp.ernet.in
Joined the department in: October, 2009

Sudip Roy *received B.Sc. (Honors) in Physics and B.Tech. in Computer Science and Engineering from the University of Calcutta, Kolkata, in 2001 and 2004, respectively, and M.S. in Computer Science and Engineering from Indian Institute of Technology Kharagpur, in 2009. He is currently pursuing his Ph.D. in Computer Science and Engineering at Indian Institute of Technology Kharagpur. His research interests are in the area of algorithms for computer-aided design of digital microfluidic biochips.*

Supervisor: Prof. Partha P. Chakrabarti and Prof. Bhargab B. Bhattacharya (ISI Kolkata)

Algorithms for Automatic Sample Preparation of Biochemical Fluids in Digital Microfluidic Biochips

Microfluidic-based biochips are recently emerged technologies and are soon revolutionalizing clinical diagnostics and other biochemical laboratory procedures (bioprotocols or bioassays) to meet the challenges of healthcare cost for cardiovascular diseases, cancer, diabetes, and global HIV crisis, etc. Research in this discipline needs the integration of many disciplines such as microelectronics, biochemistry, in-vitro diagnostics, computer-aided-design and optimization techniques, microchip fabrication technology, etc. Typically, a biochip implements one or more bioprotocols or assays on a single chip that is a few square centimeters in size [1-3].

A versatile and promising category of biochips are digital microfluidic (DMF) biochips, where discrete and independently controllable droplets of micro/nano/pico litre volume of sample/reagent fluids are manipulated on a substrate of two dimensional array of electrodes using electrical actuation (a principle called electrowetting-on-dielectric or EWOD) [1-3]. This technology offers the advantages of low consumption of expensive biochemical fluids, less likelihood of error due to minimal human intervention, high-throughput and high sensitivity, portability, increased automation, low power consumption, low cost and reliability. As each droplet (or group of droplets) can be controlled individually, these types of biochips also have dynamic reconfigurability and architectural scalability. In general, the basic fluidic operations in a DMF biochip are as follows: measuring and dispensing accurate amounts of fluids, transporting fluid droplets to appropriate locations, mixing of droplets, splitting of larger droplets into smaller ones, detection and analysis of a droplet.

Recently, many algorithms are being developed for computer-aided-design and testing of DMF biochips. In all biochips, sample and solution (mixture) preparation of biochemical fluids is very important step that can be performed on-chip or off-chip. An off-chip sample preparation increases the overall bioassay completion time. However, for fast and high-throughput

applications, sample preparation steps should be automated on-chip, i.e., integrated and self-contained on the biochip itself. Currently, we are working on the CAD problems and issues involved in the automation of on-chip sample preparation steps for a DMF biochip. Automatic sample preparation can be of two types: dilution and mixing of biofluids. Dilution of a fluid is mixing of the fluid with a buffer solution (such as water), whereas mixing of several (three or more) fluids is also performed for mixture (solution) preparation.

For on-chip sample and mixture preparation, several dilution algorithms — GAG [4], twoWayMix [5], DMRW [6] and IDMA [8], and several mixing algorithms — Min-Mix [5], RMA [7], RSM [9], have been reported to determine dilution or mixing tree (a set of 1:1 mix-split steps) from the desired concentration factor or the desired ratio of concentration factors, respectively. The existing algorithms, twoWayMix and Min-Mix [5], minimize the number of mixing steps to achieve the target concentration or ratio of concentration factors [5]. However, in a bioprotocol, waste droplet handling is cumbersome and the number of waste reservoirs should be minimized to use limited amount of sample fluid and expensive reagent fluids, and hence to reduce the cost of the biochip. Thus, waste reduction is crucial during dilution/mixing of fluids. First, we present an optimization algorithm, DMRW [6], to significantly reduce the number of generated waste droplets compared to twoWayMix [5]. Next, we design another improved algorithm, IDMA [8], that optimizes the usage of intermediate droplets generated during dilution process to reduce the numbers of input droplets required and that of waste droplets generated. An integrated scheme is presented for choosing the best waste-aware dilution algorithm among these three methods for a target concentration. We present a novel algorithm for automatic mixture (solution) preparation, referred as ratioed mixing algorithm (RMA) [7] that is more layout-aware compared to Min-Mix [5].

References

[1] K. Chakrabarty and T. Xu, “Digital Microfluidic Biochips: Design and Optimization”, CRC Press, 2010.

[2] R. B. Fair, “Digital Microfluidics: Is a True Lab-on-a-Chip Possible?”, Microfluidics and Nanofluidics, Vol. 3, March 2007.

[3] M. Abdelgawad, and A. R. Wheeler, “The Digital Revolution: A New Paradigm for Microfluidics”, Advanced Materials, Vol. 21, 2009.

[4] E. J. Griffith, S. Akella, and M. K. Goldberg, “Performance Characterization of a Reconfigurable Planar-Array Digital Microfluidic System,” IEEE Trans. Comput.-Aided Design Integr. Circuits Syst., vol. 25, no. 2, pp. 345–357, 2006.

[5] W. Thies et al., “Abstraction Layers for Scalable Microfluidic Biocomputing”. Natural Computing, Vol. 7, pp. 255–275, 2008.

[6] S. Roy, B. B. Bhattacharya, and K. Chakrabarty. Optimization of Dilution and Mixing of Biochemical Samples using Digital Microfluidic Biochips. IEEE TCAD, 29(11):1696–1708, 2010.

[7] S. Roy, B. B. Bhattacharya, P. P. Chakrabarti, and K. Chakrabarty. Layout-Aware Solution Preparation for Biochemical Analysis on a Digital Microfluidic Biochip. In Proc. of the IEEE VLSID, pages 171–176, 2011.

[8] S. Roy, B. B. Bhattacharya, and K. Chakrabarty, “Waste-Aware Dilution and Mixing of Biochemical Samples with Digital Microfluidic Biochips,” in Proc. of the IEEE/ACM DATE, 2011, pp. 1059–1064.

[9] Y.-L. Hsieh, T.-Y. Ho, and K. Chakrabarty. A Reagent-Saving Mixing Algorithm for Preparing Multiple-Target Biochemical Samples Using Digital Microfluidics. IEEE TCAD, 31(11):1656–1669, Nov 2012.

Manjira Sinha
Email: manjira87@gmail.com , 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 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 a 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, i.e. which word to use to describe a concept, 2. This layer will analyse 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.

Soma Saha
Email: somasaha45@yahoo.co.in
Joined the department in: July 2009

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.*

Supervisor: Prof. Rajeev Kumar, Prof. Arobinda Gupta

On Quality Improvement of a few Multi-Objective Combinatorial Optimization Problems with Hybridization Approach

Performance measurement is a complex issue in multi-objective combinatorial search. Not a single metric is superior in terms of all performance issues like coverage of solutions to the Pareto front, diversity across Pareto front, etc. Monitoring performance metrics on Pareto front is a step towards the improvement of quality of solutions. Having a set of test functions and metrics which could un-ambiguously monitor the performance of Multi-Objective Combinatorial Optimization (MOCO) problems is a challenging area of research. The scope of hybridization with EA approach in MOCO field is widely open due to small amount of research done with this approach.

We aim to devise a way to hybridize MOEA which improves quality of solutions for a set of MOCO problems and assess the performance across the solution sets.

On Quality Improvement of Bounded-Diameter MST Instances with Hybridization of Multi-Objective EA

We have recasted a few well-known heuristics, which are evolved for well-known Bounded Diameter (a.k.a Diameter Constraint) Minimum Spanning Tree (BDMST/DCMST) problem to a Bi-Objective Minimum Spanning Tree (BOMST) problem and then obtained Pareto fronts. A detailed analysis of Pareto fronts suggests that none of the heuristics provide superior solutions across the complete range of the diameter. In this work, we have used a Multi-Objective Evolutionary Algorithm (MOEA) approach to improve the Pareto front for BOMST, which in turn provides better solution for BDMST instances. We have considered edge-set encoding to

represent MST and then applied recombination operators having strong heritability and mutation operators having negligible complexity to improve the solutions. The analysis of MOEA solutions confirms the improvement of Pareto front solutions across the complete range of the diameter over Pareto front solutions generated from individual heuristics.

Characterization of Graph Properties for Improved Pareto fronts using Heuristics and EA for Bi-Objective Graph Coloring Problem

Bi-Objective Graph Coloring Problem (BOGCP) is a generalized version in which the number of colors used to color the vertices of a graph and the corresponding penalty which incurs due to coloring the end-points of an edge with the same color are simultaneously minimized. We have analyzed the graph density, the interconnection between high degree nodes of a graph, the rank exponent of the standard benchmark input graph instances and observed that the characterization of graph instances affects the behavioral quality of the solution sets generated by existing heuristics across the entire range of the obtained Pareto fronts. We have used Multi-Objective Evolutionary Algorithm (MOEA) to obtain improved quality solution sets with the problem specific knowledge as well as with the embedded heuristics knowledge. To establish this fact for BOGCP, hybridization approach is used to construct recombination operators and mutation operators and it is observed from empirical results that the embedded problem specific knowledge in evolutionary operators helps to improve the quality of solution sets across the entire Pareto front; the nature of problem specific knowledge differentiates the quality of solution sets.

Hybridization with EA for Solving Sudoku Puzzles

A general Sudoku puzzle is composed of an n^2 x n^2 board which is divided into n^2 number of n x n sub-grids. The original board has some of the squares filled with the digits from 1 to n and solving a feasible puzzle requires the completion of filling the empty squares of the board so that each row, column and each n x n sub-grid contains each of these digits exactly once. In this work, we have proposed a hybridized EA approach that tries to solve the Sudoku puzzles irrespective of the complexity level of the given puzzles and rate the given puzzle accurately.

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.

Prasenjit Mondal
Email: prasenjitm@cse.iitkgp.ernet.in
Joined the department in: January 2009

Prasenjit Mondal *received a M.Sc. degree in Computer Science from Vidyasagar University, Midnapore in 2005, and an M.Tech. degree in Computer Science and Engineering from Haldia Institute of Technology, Haldia in 2008. From July 2008 till November 2011, he worked in Telemedicine Project, IIT Kharagpur, as a Junior Project Officer. From December 2011 till now, he is working in Document Image Analysis Project. 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 Medical Image Processing, computer vision and pattern recognition.*

Supervisor: Prof. Jayanta Mukhopadhyay and Prof. Shamik Sural

Analysis of Brain Magnetic Resonance Images

Magnetic resonance (MR) imaging is a powerful medical imaging technique commonly used to capture information about soft tissues within the human brain anatomy at a high resolution. Automatic labeling and segmentation of different objects in brain MR images is a challenging task in medical image processing. It has various applications in medical image analysis such as, precise boundary detection of different structures (for example, ventricles, cerebrum, cerebellum, etc.), identifying brain tumors and other lesions, 3D rendering of organs, etc.

Due to the complexity of the anatomic structures of the human brain, segmentation of the MR images is a nontrivial problem. Appropriate segmentation of brain components can help researchers and physicians to understand and analyze the structure and function of the brain. For automatic labeling and segmentation, it is needed to understand shape and size of the anatomical structures present in the MR images. It has been pointed out earlier why the existing segmentation methods have lower success rate compared to human expert observers on clinical quality images, such as, MR and CT images. One of the main reasons of the limitations is that the existing methods do not use sufficient amount of prior knowledge about the segmentation problem. Also, they do not consider the three-dimensional or temporal context in the process of segmentation.

We have proposed a method for alignment of human brain magnetic resonance (MR) image sequences in the brain based on a 3D human brain model (triangulated mesh). The model-guided alignment of an MR image sequence, in this work, is defined as the process of mapping a sequence of MR images into corresponding cross-sections of a human brain model. The brain model is composed of four components, namely, cerebrum, cerebellum, brain stem and pituitary gland which are represented by four different colors. Synthesized image sequences (cross-sections) are extracted from the model at regular intervals for sagittal and coronal views as done in MR imaging. The cerebellums are segmented from the sequence of MR images by using the method of active contouring and their sizes are determined. The areas of the cerebellums are computed from the cross-sections using the color information. To obtain the optimal synthesized cross-section sequence corresponding to the series of MR images, an efficient dynamic programming based computational technique has been developed that uses the normalized sizes of cerebellum in both the MR image sequences and the cross-sections. A major application of the proposed algorithm is that the alignment information can be used as a knowledge base during the automatic labeling and segmentation of different objects in the brain MR images.

Reconstruction of a 3D brain volume from its corresponding 2D image slices is a challenging task. Although investigation of clinical data is mainly based on 2D MR image visualizations, reconstruction of a 3D volume from these 2D images is essential for a complete analysis of anatomical structures. A common and straightforward method of volume reconstruction from an MR image sequence in either sagittal, coronal or axial view, is to independently interpolate the co-registered MR images onto the target grid and average the interpolated images. However, direct 3D reconstruction by stacking successive low-resolution sections suffers from blurs and distortion. Usually, brain MR images are acquired in sagittal, coronal and axial views. The acquired images do not span the entire brain. So, the volumes reconstructed independently from each of these views do not cover the whole region of the brain. On the other hand, if multiple views (sagittal, coronal and axial) are taken together for volume reconstruction, it covers greater portions of the brain.

Based on the anatomical model-guided alignment procedure, high resolution 3D MR images of the human brain are reconstructed from low resolution MR image sequences acquired in sagittal, coronal and axial views. In this work, resolution refers to inter-slice gap between two cross-sections along any view. The algorithm uses image interpolation as the basis of volume reconstruction. It works in different stages. At first, the brightness and contrast of the MR images in different views are normalized based on the repetition time (TR) and echo time (TE) used during the MR imaging. Alignment of MR image sequences in different views is performed based on a standard 3D human brain anatomical model. Based on the alignment information, the spatial resolution of the MR images in all of the three views is normalized. Furthermore, a technique using normalized cross-correlation has been applied to refine the alignment process. Finally, the high resolution volume of the brain is reconstructed by interpolation based on inverse distance weighing. The proposed volume reconstruction scheme shows promising results producing good quality of the reconstructed volume images. As an application of the reconstructed higher resolution MR images, it is possible to study smaller structures of brain, e.g., a lesion within a reconstructed volume.

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

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

Supervisors: Prof. Chittaranjan Mandal and Prof. Dipankar Sarkar

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

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

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

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

Hence, we have formulated an algorithm to translate a PRES + model into an FSMD model and use the existing FSMD equivalence checker. It is to be noted that the timing constraints are inconsequential for demonstrating data transformation equivalence between the behaviours which allows us to perform equivalence checking using FSMDs. However, translation of a PRES+ model into the corresponding FSMD model encounters state explosion because the method essentially involves parallel composition of the concurrent transitions in PRES+. Moreover, the state explosion problem is further aggravated due to various possible interleavings of the concurrent transitions, which may come into play when timing analysis is addressed. Therefore, we have formulated a direct equivalence checking between two PRES+ models. In this direct equivalence checking method we have captured the computation of a PRES+ model at some out-port as the concatenation of parallel paths. Then using the path equivalence between the original and transformed PRES+ models, we have devised the equivalence checking calculus. In this equivalence checking method, there are some sophistications needed, such as path extension. However, unlike strictly sequential control flow of FSMDs, PRES+ models capture the concurrent control flow more vividly; exploring this feature the overhead of path extension has been avoided using a modified path decomposition of the PRES+ model.

A future work will be a comparative study of the three equivalence checking methods, one via translation from PRES+ models to FSMDs and checking equivalence of the translated FSMDs and the two methods checking equivalence of PRES + models directly. Specifically, we intend to address code motion validation for this comparative study. Next we aim at enhancing the PRES+ equivalence checker for time optimizing transformations and also loop transformations.

References:

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

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

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

Rajib Ranjan Maiti
Email: rajib.maiti@gmail.com
Joined the department in: July 2009

Rajib Ranjan Maiti *received a B.Sc. (H) degree in Computer Science from Vidyasagar Univeristy, Paschim Medinipur in 2001, an M.C.A degree from Biju Patnaik University of Technology, Orissa in 2004, and an M.Tech. degree in Computer Science and Engineering from Indian Institute of Technology, Kharagpur in 2008. From June 2008 till June 2009, he worked in Magma Design Automation (India) Pvt. Ltd. as an associate member of Technical Staff. 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 Mobile Opportunistic Networks and Time-Varying Network.*

Supervisor: Prof. Niloy Ganguly and Prof. Arobinda Gupta

Improving the Performance of Routing and Broadcasting in Delay Tolerant Networks

Delay Tolerant Networks (DTNs) are characterized by the unavailability of end-to-end path between source and destination most of the time due to node movement. The communication in DTN is opportunistic since the message is passed only when the devices, carried and/or controlled by humans, are in each other's transmission range. Therefore, the meeting frequency is primarily controlled by the movement patterns of the humans. In this direction, the problem of providing efficient routing and broadcasting in DTNs in practice will be addressed in this work.

At first, the effect of using directional antennas for routing and broadcasting in DTNs with existing models of human mobility have been investigated. However, the existing models can not satisfy a number of certain properties reported from various real world trace analysis. Also, the properties considering which the state-of-art models are built upon are not standardized. Therefore, the present focus of this work is to, first, list out a set of important properties and then, characterize their impact on protocols in DTNs. Preliminary investigation on trace analysis reveals that humans meet their neighbors and colleagues repeatedly and periodically. This motivates me to apply the techniques of temporal network theory to design efficient protocols

under practical mobility patterns. Subsequently, a theoretical framework will be developed to analyze the effect of temporal properties of human mobility patterns on the protocols.

The primary objective of this thesis is to improve the performance of the DTN protocols. The performance of DTN protocols is primarily determined by the mobility patterns of the agents. Recent studies on human mobility patterns reveal the following observations: (i) the popular places emerge from individual travel spots in any large geographic location and these popular places are at a certain distance range, and (ii) humans have repetitive contact patterns with neighbors and colleagues. The former observation motivates the use of some long range contacts among agents in different places to efficiently spread a message. Directional antenna (DA) which may be placed in mobile devices along with regular Omni-directional antenna (OA) can help in creating such contacts. The latter observation indicates that the message spreading can be achieved in an efficient way instead of commonly used probabilistic methods. In this connection, the following objectives have been identified:

1. Improving the primary network services in DTN using DAs: The goal is to analyze the impact of using DAs for message transfer in DTNs. Initially the message transfer among agents is carried out using epidemics. Also, I have investigate the impact of placing DAs depending on the mobility behaviors of the agents. Subsequently, I plan to propose an improved DTN message spreading protocol using DAs.
2. Analyzing the temporal behaviors of DTNs: The goal is to investigate the effects of the temporal properties of human mobility patterns on DTN protocols. Preliminary investigation shows that an efficient routing algorithm may developed in some DTN scenarios where agent-agent contacts are repeated at regular intervals. Subsequently, I plan to design an efficient routing and broadcasting protocol for DTN.
3. Characterizing the impact of the mobility properties of humans on DTNs protocols: Here the goal is to understand various properties- statistical and social – present in human mobility patterns and characterize their impact on the performance of the protocols. This will help to predict the impact of a new property on a set protocols in DTNs.

The works till now have completed the investigation of the impact of using DA on the performance of routing and broadcasting in DTNs in presence of practical mobility models. It has been found that the use of even a small percentage of DAs along with OA, placed randomly, can improve the performance of both routing and broadcasting.

The work done in the direction of mobility analysis shows that the properties of human movement can be organized into layers. It is seen that there are some properties which are less important in one scenario, but have significant impact on the protocol performance in other scenarios. Also, incorporating temporal properties of human movement can lead to design efficient routing protocol for some DTNs.

Chhabi Rani Panigrahi
Email: chhabi@cse.iitkgp.ernet.in
Joined the department in: July 2009

Chhabi Rani Panigrahi *received her Masters in Computer Application from Berhampur University, Odisha in 2000 and an M.Tech. degree in Computer Science and Engineering in 2007. She worked in RS software Pvt. Ltd., Bangalore as a software development engineer from August 2000 till June 2001. From July 2001 to till date, she has been working as a faculty in the Department of Computer Science and Engineering at Seemanta Engineering College (under BPUT), Odisha. 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 Software Engineering, Program analysis and Testing of object-oriented programs.*

Supervisor: Prof. Rajib Mall

An Approach to Prioritize the Regression Test Cases of Object-Oriented Programs

Regression testing involves rerunning relevant test cases from existing test suite to build confidence that there is no unintended side-effects due to changes made to a software. A naive approach would be to run the entire test suite after every change. This is usually costly, wasteful of resources, and requires unduly long time. To overcome this problem a large number of regression test selection (RTS) techniques have been proposed. However, RTS techniques often select significant number of test cases even for small changes made to a program. Researchers have attempted to make regression testing more effective by developing various approaches such as test suite minimization (TSM) and test case prioritization (TCP). These techniques usually target to reduce the cost or improve the effectiveness of regression testing.

Regression TCP techniques provide a method to order test cases according to certain criteria, so that the highest priority test cases can be executed earlier in a regression testing session. Further, when it is possible to execute only a few test cases, the most fault-revealing test cases can be executed. Regression TCP techniques usually target to order test cases based on the rate of fault detection or the rate of code coverage. Most of the regression TCP techniques proposed in the literature were developed in the context of procedural programs. These existing regression TCP techniques do not work satisfactorily for object-oriented programs, because these do not consider

the implicit dependencies that arise due to object-relations. Binder pointed out that in object-oriented programs methods tend to be small and simple [1]. Therefore, the programming complexities move from intra-procedural to inter-procedural aspects. Therefore, it can be assumed that consideration of dependencies arising on account of object-relations in regression test prioritization is important.

In this context, we have used a program model that represents the object-relations in an object-oriented program in addition to the traditional program dependencies. Again a test case which covers higher number of affected nodes in the dependency model has a higher chance to detect an error(s) than a test case which covers less number of affected nodes. Based on the above fact, we propose a regression TCP technique that prioritizes test cases according to the number of affected nodes covered by a test case in the dependency model of an object-oriented program.

References:

1. R. V. Binder. “Testing Object-Oriented Systems: Models, Patterns, and Tool”s. Addison-Wesley, (2003).

Chester Rebeiro
Email: chester@cse.iitkgp.ernet.in
Joined the department in: July 2009

Chester Rebeiro *received his MS (2009) degree in Computer Science and Engineering from IIT Madras and BE (1998) in Instrumentation and Electronics from Bangalore University. From July 1999 to May 2009 he worked for the Centre for Development of Advanced Computing. Since May 2009, he is a research scholar and a senior research fellow in the Department of Computer Science and Engineering, IIT Kharagpur. His research interests are in Cryptography and Cryptanalysis, Computer Architecture, and VLSI*

Supervisor: Dr. Debdeep Mukhopadhyay

Secure Hardware Architectures for Cloud Infrastructures

Over the next decade, as Cloud Computing becomes a commodity, Cloud Service providers will compete on service quality and price. In order to increase the percentage of IT operations that will be moved from in-house IT to Cloud Service providers and their Data Centers, service providers will need to ensure the security of a customer's applications and the integrity of its data from other applications co-located in the same Cloud. As part of this effort, the ability to protect against side channel attacks will be an important component. A side channel attack is an attack based on a system's physical implementation rather than any weaknesses in the encryption algorithm itself. Data Centers are especially vulnerable to such attacks because the attacker may reside on the same physical machine as the application being attacked.

Current countermeasures for side-channel attacks follow a *find-and-patch* methodology, where a security vulnerability if found, is patched in the application itself. However, several of the vulnerabilities stem from the underlying hardware. For example, attacks on systems have been demonstrated using inherent vulnerabilities present in hardware components such as cache-memories, branch-prediction units, hyper-threading units, etc. There are several drawbacks of countering these attacks at the application layer. First, most of these 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 the

performance and energy requirements of the system. Second, there exists no panacea that can plug all attacks. A countermeasure to prevent an attack may lead to new attack techniques, which use the same vulnerabilities.

The aim of this research is to tackle the root cause of these vulnerabilities; by plugging them in the hardware itself instead of the application layer. This can be made feasible due to the rapid growth in Silicon technology, resulting in more transistors put on chip. Such countermeasures applied in the hardware would be a safeguard for all applications running on the system and thereby have less impact on the performance and energy requirements. Further, since the vulnerabilities are plugged at the root, all attacks that utilize these vulnerabilities are prevented.

Although ideas of securing systems at the hardware itself, have been floated for several years such as by Dan Page in 2005, only recently have practical realizations of this idea been made. For example in random caches, non-monopolizable caches, and time fuzzing. While the former two works strictly to plug vulnerabilities in cache-memories, the latter aims at preventing all attacks that time micro-architectural events. We plan to expand these works and not being restrictive to cache memories and timing. As a first step we plan to develop a metric which can be used to quantify the vulnerabilities of architectural and micro-architectural components. We will then use this metric to identify and order the components in terms of their vulnerabilities, and then develop new algorithms and techniques to plug the vulnerability. The hope is to develop a computer system with inherent protection against side-channel attacks.

Sourav Kumar Dandapat
Email: sdandapat@cse.iitkgp.ernet.in
Joined the department in: July 2009

Sourav Kumar Dandapat *received a B.E. degree in Computer Science from Jadavpur University in2002 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

Applications and solutions for next generation Wireless Internet

Wireless Internet provides anytime and anywhere connectivity to its users. Increasing numbers of users (approximately 2.3 billon users currently), continuous demand for better quality as well as the need for providing new innovative applications make research in the field of wireless network very challenging. There are lots of important areas where contributions need to be made – out of which we are concentrating on two problems: (a) Developing smart association control scheme and (b) Developing a content delivery system for wireless network which in effect can reduce overall traffic congestion.

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 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.

Content Distribution in Wireless Network

Due to the availability of cheap handheld devices and ubiquitous wireless connectivity, a huge demand for content has been noticed from wireless users. In year 2010, total wireless Internet traffic is 37% of overall Internet traffic and it has been predicted by 2015, it will cross 50%. This fact motivates to re-think for some new content delivery technique for wireless network which can reduce network traffic. To reduce the Internet traffic, one possible solution is to distribute the content utilizing some underutilized network resource (like WiFI in road network) for that local area. We envision cities where networking infrastructures, such as Wi-Fi access points (AP), will be equipped with storage capabilities. We propose to utilize the storages as a large distributed video cache. The key challenge arises from the fact that the mobile tablet would not be able to download the entire movie from any single AP. Nonetheless, we show that the APs could be appropriately populated with video “chunks”, such that mobile device on move can almost always get the needed chunk, just-in-time for video playback. Our system minimizes replication of video chunks, offering citizens with far greater number of videos to watch. We believe that such a video service could benefit cellular networks, by offloading their traffic to a sizable extent. In this work, we take a step into exploring such a city-wide content distribution service, and address one piece of the puzzle – efficient content storage.

Kamalesh Ghosh
E-mail: 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 tradeoff 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.

Satya Gautam Vadlamudi
Email: satya@cse.iitkgp.ernet.in
Joined the department in: August 2009

Satya Gautam Vadlamudi *received a B.Tech. (Hons.) degree in computer science and engineering from the Indian Institute of Technology (IIT) Kharagpur, Kharagpur, India, in 2008. From June 2008 to July 2009, he was a Software Engineer with Google India Pvt. Ltd., Bangalore, India. Since August 2009, he has been a Research Scholar with the IIT Kharagpur. His areas of interest include AI, data mining, design and validation of dependable systems, and algorithm design. He received the Pratibha Award from the Government of Andhra Pradesh (2004), the MCM Scholarship from the IIT Kharagpur (2004-2008), and the SAP Labs Doctoral Fellowship (2010-present) for his academic and research works. He is a graduate student member of IEEE.*

Supervisor: Prof. Partha Pratim Chakrabarti

Design and Validation of Dependable Systems

Embedded control systems are widely used in several domains such as aeronautic, aerospace, automotive, nuclear, medical, etc. The components often carry out highly safety-critical operations, which makes it extremely vital for them to be fault-tolerant. Faults such as ECU (Electronic Control Unit) failure, link failure were well studied.

We proposed the quality-fault model where we consider faults such as small amounts of shift, noise, and spikes on different signals of the electronic control system simultaneously (which can happen due to sensor faults, submicron chip technologies being used, etc.), and studied the behaviour of the system over a period of time for any unacceptable deviations from golden behaviour. We have proposed an efficient framework for finding the counterexamples (violating the given fault-tolerant requirements) which does static analysis on the network of abstract models of each component of the system.

Further, we have proposed a methodology for finding critical components in a given embedded control system which is sensitive to quality-faults. It takes the counterexamples generated by the previous method as input and exhaustively traverses the given control model to find the components where the input to output error induction ratio is the highest/crosses the given limit. These components are reported back to the designer to re-design them such that they are less sensitive to quality-faults.

We have also proposed formal methods for determining whether a set of components having given reliability certificates for specific functional properties are adequate to guarantee desired

end-to-end properties with specified reliability requirements. We solved this problem by mapping it to the monotone multi-dimensional array search problem for which we have proposed an efficient divide and conquer algorithm. Future directions include, developing more efficient and higher coverage fault-tolerance analysis methods/frameworks, methods to guarantee/verify end-to-end reliability of systems, and to explore reconfigurable architectures for achieving fault-tolerance at low cost.

Spatio-Temporal Data Mining

Spatio-temporal data mining of mobile user data such as the times series of locations of all individuals over a period of time is extremely useful for mining several interesting patterns. Groups, events, trajectories, hotspots, etc. have been mined in the past for using in social-network analysis, traffic modeling, crime investigation, etc.

We attempt to model novel queries which can be of use, such as, finding groups that cover maximum number of users, finding a mobility model that best fits a person or a group, finding large sized gatherings, such as, a cricket match, or a wedding, etc. We aim to develop methods which can answer such hard queries quickly (seconds/few minutes), and which can scale over large number of users and large time periods.

We solved the problem of finding K groups which cover maximum number of users, which maps to the maximum coverage problem with a very large number of input sets (O(millions)). Efficient anytime algorithms were proposed which do not mine all the groups from the data apriori saving time and resources but intelligently explore the most promising areas of search space with dynamic self online feedback to give good performance.

Also, the mobility data itself is limitedly available due to privacy reasons, therefore, a realistic mobility simulator is also developed by efficiently capturing the spatio-temporal group behavior of humans, for testing the mining methods.

Heuristic Search

Heuristic search methods based on A* and beam search are widely used for solving several optimization and path planning problems. Due to large search spaces of the problems, anytime methods were developed for producing good quality solutions quickly. However, such anytime algorithms run out of memory when dealing with large sized search spaces.

We proposed a memory-bounded anytime heuristic search method called MAWA* (Memory-bounded Anytime Window A*) which works within the given amount of memory (should be at-least sufficient to hold all nodes of a single path from the start node to a goal node, which is usually very small), and still gives very good anytime performance. MAWA* is developed by intelligently combining AWA* (an anytime algorithm) and MA* (a memory-bounded algorithm). Also, it guarantees to terminate with an optimal solution. We have also developed a new anytime algorithm, called Anytime Column Search, that is not memory-bounded but which is effective in solving many practical problems such as, robotic arm trajectory planning, AI based games, combinatorial optimization, etc. The algorithm is one of the simplest anytime algorithms with good performance. Future directions include, developing parallel anytime algorithms, contract search algorithms (given a fixed amount of time, memory—get the best possible solution), etc.

Rishiraj Saha Roy
Email: 10cs9401@iitkgp.ac.in
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 January 2010, 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.*

Supervisors: Prof. Niloy Ganguly (IIT Kharagpur) 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.

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.

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 with focus on testing of Network-on-chip based architectures. His other research interests are FPGA based system design, developing open source EDA applications for VLSI design. 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

Manufacturing test of embedded memories is an essential step in the Systems-on-Chip (SoC) production that screens out the defective chips and accelerates the transition from the yield learning phase to the volume production phase of a new manufacturing technology. Built-in Self-Test (BIST) is establishing itself as an enabling technology that can effectively tackle the SoC test problem. However, unless consciously implemented, main limitations of BIST lie in elevated power dissipation, area overhead, potential performance penalty and increased testing time, all of which directly influence the cost and quality of manufacturing test.

The objective of this research is to propose improved BIST approaches for memories embedded in SoCs targeting low area, power and low testing time. The approaches proposed in the research have explored the following directions to gain improvements:

Architecture: It should be distributed to allow hardware sharing. It should choose the interconnect judiciously to avoid routing congestion and reduce area overhead. A balance of both parallel and serial testing techniques may be best. State-of-the-art SoCs include many types of memory cores and as VLSI technology moves below 100 nm, process variations lead to different

types of defects in different memories. Thus, traditional fault testing is not sufficient to detect all memory related faults present in the SoCs. Hence, the architecture must be a programmable Memory BIST (MBIST) architecture which supports multiple test algorithms for higher fault coverage.

Test scheduling algorithms: Since test scheduling under power constraints is highly interrelated to the resource sharing mechanisms used in the MBIST architecture, it is essential to develop new power-constrained test scheduling algorithms that will get the maximum usage of the available hardware resources for embedded memory testing. By carefully scheduling memory testing with tightened power constraints, the overall testing time for the SoC can be reduced.

Special design implementations: By analyzing the implementation requirements some different kind of implementation techniques should be investigated for example re-using already existing refresh technique in test process to avoid use of extra Design For Testability (DFT) logic, investigate low power DFT techniques and use them in the test of the memories.

At-speed testing: Process variations lead to such timing related defects which can only be detected if the memory is tested at functional speed. Thus, the proposed MBIST techniques must ensure at-speed test operation for maximum fault coverage.

Although most of the above directions have been used separately by researchers, there are no comprehensive system-level solutions for effective power constrained testing of hundreds of embedded memories (i.e., achieve high test concurrency with low overhead in DFT hardware), that exploit the specific features of SoC architectures.

We have been able to propose a solution for System-On-Chip based systems having hundreds of embedded memories which are connected using Netwok-on-Chip (NoC) based communication infrastructure. We have proposed a hybrid test approach where both the serial and parallel testing techniques can be utilized to optimize test time as well as test power. The proposed test architecture is a distributed MBIST architecture having a number of BIST controllers each of which is responsible for testing a group of heterogeneous memory cores. The groups are tested in pipeline while memories in a group are tested parallely. Re-using the NoC to act as Test Access Mechanism (TAM) brings down the area overhead as well as avoids routing congestion. An obvious question that comes up is what should be the condition for group formation and how many groups will be formed? It is expected that the number of groups that are formed is minimum so that the area overhead due to the BIST controllers is minimum. Moreover, the groupings should also ensure that the power dissipation during test is within the power budget. Thus, we have proposed a test schedule which involves a grouping technique whose aim is to group memory cores which are at same distance from a BIST controller (to avoid congestion as well as reduce test time) and that the created groups adhere to the required timing precedence relation. Then, to satisfy the power constraint, a power aware test schedule is applied on the different groups.

Subhasish Dhal
Email: 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

Abstract: RFID technology defeats bar code reader in respect to the efficient reading capability and it does not need line of sight constraint. Therefore, the objects are tagged by RFID tag which contains the information related to the object. Sometimes, the information related to an object is such that the RFID tag is unable to contain the whole. In that situation, a backend database is used to keep the relevant information. The tag only keeps the key information. RFID reader reads the key information and consults with the backend database for the detail information. The information related to the objects may be secret and hence the access needs to be secure. Therefore, security such as privacy, authentication, integrity etc is the basic requirements for RFID communication. We are focusing on the authentication issues. Authentication scheme can be extended to devise the tag searching scheme. However, this approach will be inefficient and hence need to look an efficient tag searching scheme. We propose an object searching scheme. In another work, we aim to propose a scheme which can be used to bind a number of related tags and hence tag dependency issues can be resolved in some situations. Use of multiple RFID tags in an object increases the detection rate in comparison to the single tagged object. Since, more than one tags are involved in the same object, the security such as authentication scheme needs to be revised. Our objective is to build a lightweight authentication scheme which will give maximum security in respect to the authentication to the RFID communication.

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

Kunal Banerjee *received a B.Tech. degree in Computer Science & Engineering from Heritage Institute of Technology, Kolkata in 2008. Since January 2010, he has been a research scholar in the department of Computer Science & Engineering in IIT Kharagpur. Prior to his doctoral studies, he worked as an Assistant 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. Due to increasing design complexity of such systems, designers advocate construction of an initial meta-model of the overall system which is transformed through a sequence of refinements eventually leading to the final implementation. When a more detailed design is obtained from a higher level design, it becomes necessary to ensure that the lower level design satisfies certain properties. For this task, model checking is used as the primary verification approach for embedded system design. The verification models are automatically generated from the design description of each abstraction level and the properties are checked using model checkers such as, SPIN. However, verification of a synthesizable specification is not restricted to demonstrating some liveness or safety properties only. Instead, it should establish that all the behaviours depicted by a higher level abstraction are captured by a lower level abstraction, and vice-versa. For this task, however, model checking cannot be used as it is appropriate for property verification but not for behavioural verification in its entirety. So, it is necessary to devise some efficient verification methodology that demonstrates behavioural equivalence between two descriptions. Also, it is important to develop proper abstractions for modeling such complex systems so that the relevant aspects of the behaviours are captured for verification. Our work mainly focuses on these two issues that arise during embedded system design verification.

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.

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 intend to devise a method that will be able to handle control structure modification as well as code motions across loops.

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.

Addressing Completeness Issues of an Equivalence Checking Procedure: Equivalence checking of even uninterpreted flowchart schemas is not even semidecidable (recursively enumerable). So, no equivalence checker can be complete even as a partial decision procedure; in other words, no equivalence checker can yield the answer “yes” for all equivalent inputs. However, possibly, the equivalence checking problem restricted to the subset where the applied transformations are mechanizable is decidable. Now, to prove the decidability of this subset, we can either reduce it to a decidable problem or devise an algorithm and show its soundness and completeness. The latter approach is what we intend to work upon obviously because we already have an algorithm.

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

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

Supervisor: Prof. Anupam Basu

Towards 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.

Reference

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.

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 trend towards using component-based hierarchical design approach in system development requires addressing newer system engineering challenges. Based on an overall architectural plan, large designs are built hierarchically starting from the leaf-level components and thereby gradually constructing the overall system (bottom-up). During the development phase of such component-based hierarchical systems, the designers need to guarantee four critical aspects of design, namely – *correctness*, *timing and performance*, *power intent* and *functional reliability*. A significant amount of research has been conducted on the aspects such as *design intent verification* (to ensure correctness) and *timing/performance analysis* of component-based designs. Emerging paradigm, like design intent coverage, ensures that the component-level formal specifications together guarantee the end-to-end system requirements. Moreover, the component-based complex systems of modern days are usually very time-critical and require timing guarantees from components. So for system integration, the current research also focuses on introducing new notion of overall system timing layout by specifying the time-budgeting for its constituent components. However, meeting a stringent low-power budget by efficient global power management schemes and meeting the desired level of functional reliability for the overall system are emerging issues now-a-days. This work tries to address (from architectural point of view) the following two important aspects of component-based hierarchical system design: *power intent verification* and *functional reliability analysis*.

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.

Apart from the correctness, 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. Typically, the number of global power states reachable by the global power management strategy is significantly lesser than the possible number of global power states. 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.

In addition to this, though the structural reliability of logic circuits as well as component-based embedded systems are well studied, however early analysis of the *functional reliability* of a component-based design is becoming important in high integrity systems. In our work, we present formal methods for determining whether a set of components having given reliability certificates for specific functional properties are adequate to guarantee desired end-to-end properties with specified reliability requirements. We also introduce the formal notion of *logical reliability gap* in component-based designs. This analysis opens the avenue for developing suitable procedures to bridge the functional reliability gap. Hence, there is a need to formally model the functional (logical) reliability and devise suitable techniques to determine reliability intent coverage for component-based embedded systems.

Moreover, in an embedded system development framework, the architectural level functionalities are decomposed into set of tasks to be executed (mapped) over a set of ECUs. The reliability of the overall functionality is dependent on the reliability of the executed tasks. To improve the reliability of the overall functionality, it is often necessary to re-execute certain critical tasks – thereby ensuring higher reliability through temporal redundancy. Therefore, it is necessary to develop reliability-oriented scheduling criteria for the generated tasks. In future, we try to leverage this aspect for improving the system reliability as well.

Therefore, this work, as a whole, aims to enable formal methods for addressing two important aspects of component-based designs (from the architectural perspective), namely, power intent verification and functional reliability analysis.

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

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

Supervisor: Prof. Niloy Ganguly and Prof. S. K. Ghosh

Topical Search in Twitter Online Social Network

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

One of the primary requirements for implementing topical search, on an OSN is to discover topical attributes of the users who are the primary sources of information in an OSN [1, 5]. 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].

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.

Sudipta Saha
Email: sudipta.saha@cse.iitkgp.ernet.in
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

Information Management in Unstructured and Challenged Networks

Information management services on networks, such as search and dissemination, play a key role in any large scale distributed system. One of the most desirable features of these services 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. Using results from analytical studies done in the past on K-random walk based algorithm, we identify that redundancy quickly increases with increase in the *walker-density*. Based on this postulate, we design a very simple distributed algorithm which dynamically estimates the *walker-density* and thereby carefully proliferates walkers in sparse regions. We use extensive computer simulations to 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.

This research also focuses on understanding the buffer-assisted information dissemination process in Delay Tolerant Networks (DTN) which generally lack continuous network connectivity. These networks (also termed as challenged networks) are often augmented with message buffers (i.e., relay points such as 'throwboxes') in order to effectively increase the contact frequencies between the mobile nodes. This infrastructure of the buffers plays an important role in disseminating information in the network. Not only the achieved coverage, i.e., the number of nodes to which a message could be delivered in an information dissemination process in DTN, but also the incurred overhead in the process is directly related to the buffer

time, i.e., duration of time a particular instance of a message resides in the installed buffers. Therefore, the buffer times are restricted which imposes limitation on the maximum coverage that can be achieved. In addition, the application of store-carry-forward paradigm as well as existence of complex human mobility patterns incorporating variants of preferential selection of the places to be visited next, make it hard to leverage on traditional mathematical tools to analytically solve the problem of finding optimal buffer time for a desired coverage under a predefined cost limit. In this research work we propose a bipartite network (BNW) model for the DTN and show that the time evolution of the former matches with the dynamics of the latter. Specifically, we demonstrate that, the limitation imposed by a given buffer time in DTN can be modeled by suitably thresholding the *one-mode projection* of the corresponding BNW. Exploiting this correspondence between DTN and BNW, we also derive a closed from equation to estimate the coverage. The elegance of this bipartite construction is that minor variations in the DTN dynamics do not affect the preamble of the construction. In summary, we outline a method to calculate the optimal buffer time for a desired coverage to cost ratio.

We also exploit the existing theoretical backbone of bipartite networks to understand the inter-group information flow in various online social systems. In such systems, users with common affiliations or interests form social groups for discussing various topical issues. We study the relationships among these social groups, which manifest through users who are common members of multiple groups, and the evolution of these relationships as new users join the groups. Focusing on a certain number of the most popular groups, we model the group memberships of users as a subclass of bipartite networks, known as *Alphabetic Bipartite Networks* (α-BiNs), where one of the partitions contains a fixed number of nodes (the popular groups) while the other grows unboundedly with time (new users joining the groups). Specifically, we consider the evolution of the *thresholded projection* of the user-group bipartite network onto the set of groups, which accurately represents the inter-group relationships. We propose and solve a preferential attachment based growth model for evolution of α-BiNs, and analytically compute the degree distribution of the thresholded projection. We further investigate whether the predictions of this model can explain the projection degree distributions of user-group networks derived from several real social systems (Livejournal, Youtube and Flickr). The study also shows that the inter-group network is tightly knit, and there is an implicit semantic hierarchy within its structure, that is clearly identified by the method of thresholding.

In this research we also try to enhance the theoretical base of the bipartite networks. Specifically, we aim on mathematically analyzing the size and the exact structure of the components found in the *thresholded one-mode projection* of the alpha-bipartite networks for the full spectrum of the possible threshold values. We exploit the theory of random-threshold-graphs to achieve this.

Subhadip Kundu
Email: subhadip@iitkgp.ac.in
Joined the department in: July 2010

Subhadip Kundu *received Bachelor of Technology Degree (B.Tech) from West Bengal University of Technology in Electronics and Communication Engineering in the year 2007. He received MS degree from Indian Institute of Technology Kharagpur in 2010 from Electronics and Electrical Communication Department. His MS research topic was Low Power Testing. Currently he is pursuing PhD from Computer Science and Engineering Department, Indian Institute of Technology Kharagpur. His current areas of research are: Fault diagnosis in digital VLSI system, Power and thermal aware testing. He has published more than 15 international conference and journal papers in this domain.*

Supervisor: Prof. Indranil Sengupta and Prof. Santanu Chattopadhyay

Fault Diagnosis in Digital Systems

When a VLSI circuit fails a test, diagnosis is the process of narrowing down the possible locations of the defects. Fault diagnosis is extremely important to ramp up the manufacturing yield especially for 90 nm and below technologies where physical failure analysis machines become less successful due to reduced defect visibility by the smaller feature size and larger leakage currents. Diagnosis helps to reduce the product debug time as well. By reducing the candidate locations down to possibly only a few, subsequent physical failure analysis becomes much faster and easier when searching for the root causes of failure.

A failure can occur in a circuit due to the defects present in the logic circuit or in the scan chains. While many defects reside in the logic part of a chip, defects in scan chains are becoming more and more common, as typically 30%-50% logic gates impact the operation of scan chains in a scan environment. Logic and scan chain diagnosis are the two main fields of diagnosis research. In this work, we have considered both the problem of logic and scan chain diagnosis and attempt to find a suitable diagnosis methodology to assist in finding out the defects that possibly caused the circuit to fail.

The followings are the major objectives of the research work:

Multiple fault diagnosis in combinational logic circuit

With the ever-increasing complexity of VLSI circuits, multiple faults have now become a reality. Almost all the conventional fault diagnosis methods are based on single fault simulation. But a single fault injection cannot manifest the effect of multiple faults that are present in the actual

failed circuit. Thus, in this work, we propose to inject multiple faults simultaneously, and perform an effect-cause analysis to find the possible list of faults. Since, the number of faulty sites is unknown, multiple fault simulation algorithms are inherently exponential in time. So, to cover this exponential search space, we propose to use a Particle Swarm Optimization (PSO) algorithm for finding suitable solutions.

A diagnosability metric for test set selection

The primary focus of a diagnosis algorithm is to accurately narrow down the list of suspected candidates. For that, all the diagnosis algorithms depend on the failure information produced by the tester. Some diagnosis algorithms also use the pass patterns to narrow down the list further. Overall, the backbone of any diagnosis algorithm is the test set in use. Thus, for any diagnosis algorithm, the effectiveness will depend on the test set in use. If the test set used is not good enough to distinguish between fault pairs, the diagnosis algorithm can never be able to distinguish between a good number of faults. This problem leads us to find a metric which can characterize test sets in terms of their diagnostic power. In literature, several methods have been proposed for assessment of the diagnostic power of a test set. Though the methods are accurate in nature, the bottleneck is the space and time complexity. In this work, we propose to find out a metric to describe diagnostic power of a test set efficiently.

Multiple chain failure in extreme space response compaction environment

Due to limited tester memory, test response compaction for large circuit has now become a necessity. With the space compactor, the number of scan chains is much larger than that of traditional scan designs, thus the probability of having multiple scan chain failures is even higher in a modern scan compression design than traditional scan design.
When space compactors are used, internal scan chains are not observed directly at the output channel. The reduced observability of internal scan chains and the interaction between them can adversely impact scan-based diagnosis. Thus, we propose to develop a suitable methodology for diagnosis of multiple chain failure in response compaction environment.

De-compressor Side Masking: A DFD for Scan Chain Diagnosis

Volume Diagnosis is extremely important to ramp up the yield during the IC manufacturing process and thus reduces the time to market and product cost. However, the process is time consuming and requires appropriate test equipments, supporting diagnosis infrastructure. The limited observability due to test response compaction negatively affects the diagnosis procedure. Hence, in a compaction environment, it is important to implement Design For Diagnosis (DFD) methodology to restore diagnostic resolution. In this paper, a novel DFD technique which makes the faulty chains to behave as good chains during loading, has been proposed. As a result, the errors introduced in the responses, must occur during unloading of the scan chains. Diagnosis can then be performed by directly comparing the actual and expected responses without any fault simulation - leading to significant reduction in time. The proposed DFD technique requires negligible hardware overhead and does not require any special diagnostic patterns. It can also handle failure at multiple chains at the same time.

Ruchira Naskar
Email: ruchira.naskar@gmail.com
Joined the department in: July 2010

RuchiraNaskar *received a B.Tech degree in Information Technology from West Bengal University of Technology in 2008, and an M.Tech. degree in Information Technology from IIT Kharagpur in 2010. Since July 2010, she has been a Ph.D. scholar in the department of Computer Science & Engineering in IIT Kharagpur. Her research interests are Digital Forensics, Multimedia Security and Cryptography.*

Supervisor: Dr. Rajat Subhra Chakraborty

Multimedia Content Protection through Reversible Watermarking: Theory and Implementation

Digital watermarking is the act of hiding information in multimedia data, for the purposes of content protection or authentication. In ordinary digital watermarking, the secret information, the *watermark*, is embedded into the multimedia data (*cover data*), in such a way, that distortion of the cover data due to watermarking is almost negligible perceptually. In industries dealing with highly sensitive data such as medical, military or legal industries, even the minimal data distortions are difficult to be tolerated, even if not perceptually significant. In such domains, cover information is extremely sensitive and recovery of the original cover information in an unaltered form is of utmost importance. In such cases, reversible watermarking algorithms have been found useful where by the very nature of the watermarking algorithm, the original cover data content can be retrieved exactly with zero–distortion.

An example from the medical industry will illustrate the need of reversible watermarking clearly. In hospitals Electronic Patient Records (EPRs) are used by professionals such as doctors, clinical researchers and insurance companies. Many times, the EPRs are kept embedded into medical multimedia data (such as radiographs, urograms, mammograms etc.) in form of watermark. This causes some distortion of the cover data. Moreover, patient records change over time, and this phenomenon requires the embedded EPRs to be updated from time to time. Repeated extraction and embedding of EPRs, in order to update them, causes the distortion of the

cover data to accumulate. Since such accumulation of distortion might adversely affect the quality of the image so that it becomes difficult to make the correct diagnosis, this situation is undesirable and can be improved by the use of reversible watermarking.

The last couple of decades have seen rapid growth of research interest in the field of reversible watermarking of multimedia data. Reversible watermarking is a technique used for authentication of digital multimedia data as well as distortion–free recovery of the original data contents after authentication. Primary goal of reversible watermarking is to maintain perfect integrity of the original content after watermark extraction. Amongst several reversible watermarking schemes that have been proposed till now by researchers, an overwhelming majority have been proposed for digital images.

The major goal of my Ph.D. work is to analyze, implement and evaluate reversible watermarking algorithms, theoretically as well as through simulations. Majorly I am focusing on reversible watermarking of digital images.

Sabyasachi Karati
Email: skarati@cse.iitkgp.ernet.in
Joined the department in: June 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

Algorithm Design and Implementation Issues in Cryptography

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 two new algorithms which replace square-root computations by symbolic manipulations to improve the efficiency. We did experiments on NIST prime curves to measure the speedups. We obtained a maximum speedup of above *six* 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, both achieved by a fast variant of our second symbolic-manipulation algorithm. These algorithms are practical only for small (≤ 8) batch sizes. We also port our algorithms to the NIST Koblitz curves defined over fields of characteristic 2.

Sandip Karmakar
Email: sandip1kk@gmail.com
Joined the department on: January 2011

Supervisor: Prof. Dipanwita Roy Chowdhury

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.*

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.

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

Sanjoy Pratihar *received his BTech in Computer Science and Engineering from North Eastern Hill University, Shilong, India, and received his ME 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. He has published 7 research papers in edited volumes and refereed conference proceedings.*

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.

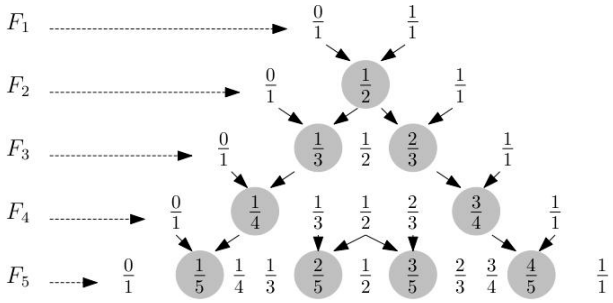
Polygonal approximation An efficient boundary representation of an object in the digital plane is done through polygonal approximation. During approximation, “reasonably collinear” straight edges are successively merged. The collinearity is tested by edge slope, which corresponds to AFT rank. If the *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].

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.

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

Tripti Swarnkar *received a MCA degree from Government Engineering College Raipur C.G. (presentaly 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 she is 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 gene expression 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 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. 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 classes. The problem is to select features; here our genes are our features that have the biggest impact on describing the results and to drop the features with little or no effect. 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 clusters, 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 finding clustering strategies to detect biomarkers, i.e. selecting features such that minimum information loss is incurred in the process, as well as minimizing the redundancy present in the reduced feature subset. The analysis of gene expression is followed by the ability to visualize, as a means of understanding the relationships between genes and treatments in an ever increasingly complex data set environment.

Joy Chandra Mukherjee
Email: joy.cs@cse.iitkgp.ernet.in
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

Design of Distributed Scheduling Algorithms 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. This information is 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 is resumed or 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.

Sudakshina Dutta
Email : sudakshina@cse.iitkgp.ernet.in
Joined the department in: July 2011

Sudakshina Dutta *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

Formal Verification is the act of proving or disproving the correctness of the algorithm in any software or hardware systems. Different aspect of modeling concurrent systems include simple case in which processes run completely autonomously to the more realistic setting where processes communicate in some way. Seemingly innocuous small concurrent programs have been known to exhibit completely unanticipated behavior that, in some cases, may lead to crashes in the critical systems. This is why different verification techniques for exhaustively checking is really required for correct execution of the concurrent systems.

Tanmoy Chakraborty
Email: its_tanmoy@cse.iitkgp.ernet.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: Dr. Animesh Mukherjee and Dr. 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.

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

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

Supervisors: Dr. Rajat Subhra Chakraborty and Dr. 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 a mathematical framework to evaluate resistance of PUF design against modeling attack.

Tanwi Mallick
Email: tanwireachesu@cse.iitkgp.ernet.in
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 Image Processing.*

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

Human Activity Tracking using Kinect

Human activity tracking and analysis have been motivated by the desire to understand human posture, pose, gestures, and gait to construct the next generation user interfaces and to build intelligence to reason from visual observations involving human beings. Most applications ranging from surveillance to communication to medical diagnostics or to robotics, deal with pronounced (walking, running, jumping etc) or subdued human activities.

Human activity tracking has been revolutionized with the introduction of Kinect – a low-cost ranging device from Microsoft. In addition to an RGB camera and an array of microphones, a Kinect has an infrared camera that captures range data for a (human) object in 3D under ambient light conditions indoor. This can then be processed to detect and track different human body motions by using the 20-joints human skeletal model.

This research deals in Human Activity Tracking, gesture & posture Identification and Interpretation from Multiple Sources of Information as provided by Kinect. It starts with low-level processing and feature extraction from sensory data that are used in high-level inferential algorithms to conclude about the state of the subjects.

Typical Kinect depth data demonstrate a few artefacts (noise) that need to be handled properly before further processing. The characteristic of these artefacts are analysed and removed from the depth map. The depth maps are then segmented to detect the human figures. Noise free depth

maps naturally lead to better segmentation results. Human figures are then tracked over the sequence of frames. In addition, skeletons are also extracted and tracked over a sequence of frames. Often independent algorithms are used for skeleton formation to alleviate the bias of the 'learned' models that dictate the third-party middleware libraries such as Kinect SDK, OpenNI , and OpenKinect. For a given sequence of depth and intensity images of a person, the goal is to estimate the full-body pose of the person at each frame, parameterized by the joint angles of the skeleton model.

Once the human figures are detected and skeletons are tracked various classification and model based learning algorithms can be used to parse gestures and pose in variety of human activities including choreography and non-verbal communication. Applications cover different Human Computer Interfaces (HCI) including tutoring, animation, medical assistance and navigation.

Anupam Mandal
Email: amandal@cse.iitkgp.ernet.in
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: Dr. 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.

Prajna Devi Upadhyay
Email: prajna.upadhyay@cse.iitkgp.ernet.in
Joined the department in: July 2012

Prajna Devi Upadhyay *received a B.Tech. degree in Information Technology from Assam University, Silchar in 2010, and an M.Tech. degree in Information Technology from National Institute of Technology, Durgapur 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 Data Mining.*

Supervisor: Prof. Sudeshna Sarkar and Prof. P.P. Chakraborty

Mining Patterns from Spatio-temporal data

We are interested in mining patterns from Spatio-temporal data. We have been working on heuristic search for finding spatio-temporal groups. We look for evaluation functions and search strategies that will enable us to efficiently find Top K groups.

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

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

Supervisor: Prof. Dipanwita Roy Chowdhury

Design and analysis of symmetric ciphers

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.

The last decade has seen competitions like the AES competition, the eSTREAM project and the SHA competition which have led to very efficient and secure designs of block ciphers, stream ciphers and hash functions respectively. Cryptanalysis has also evolved with new state-of-the-art attacks being reported. However, these standards offer very generalized solutions and may not be suitable for deployment in all sorts of environments. This precludes the need for customized solutions. In some scenarios this would imply high-throughput design while others may need a more compact design suitable for resource-constrained environments. In this work, we try to concentrate on design and analysis of such customized constructions and evaluate them in the light of both theoretical and side-channel cryptanalysis.

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, IIT Kharagpur
Collaborator Prof Soumen Chakrabarti, IIT Bombay.

Link Prediction in Social network

In link prediction (LP), a graph mining algorithm is presented 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.

Jimmy Jose
Email: jimmy@cse.iitkgp.ernet.in
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 Roy Chowdhury

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.

Ranita Biswas
Email: ranitabiswas@cse.iitkgp.ernet.in
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: Dr. Partha Bhowmick

Analysis of 3D Digital Surfaces by Number Theoretic Interpretation

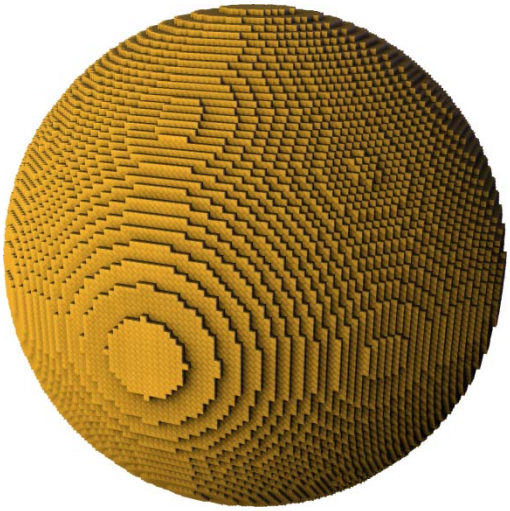
Our research is centered on *digital geometry* [1,2], which is an upcoming research specialization of *discrete geometry*. Combinatorial properties of configurations of discrete-geometric objects (e.g., points, lines, planes, circles, spheres, etc.) in the digital space are investigated in the field 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.) which are specified by integer coordinates.

The mathematical roots of digital geometry lie in *graph theory* and *discrete topology*. It deals with sets of grid points like *number theory* and *geometry of numbers*, and also with cell complexes in *discrete topology*. Some related works by Gauss, Dirichlet, and Jordan may be regarded as the historic context of digital geometry [1]. The methods of digital geometry are directly linked to the numeric computations in science and engineering, especially when the computations are directly or indirectly mapped to the integer domain. They are particularly useful to solve various problems in computer graphics, pattern recognition, and image processing.

Research work in 3D digital geometry has gained much momentum since the last decade. Several theoretical works related to 3D digital lines and digital planes done in recent time are mostly analytical and algorithmic in nature, and are mainly based on *geometry of numbers*. Till date, there has been no work related with spheres and hyper-spheres in digital space. As spheres and hyper-spheres can be conceptually thought as a dimensional extension of circles, and as

digital circles have interesting number-theoretic properties [3], we have started our research with designing a number-theoretic algorithm for generation of spheres in 3D digital space.

Currently our research focuses on digitization of Euclidean/ real spheres in 3d digital space using integer operations only. Such operations inherit from number-theoretic interpretation of the digital sphere, which, by definition, consists of all the grid points (i.e., integer points) with isothetic distance less than 1/2 from the surface of the corresponding real sphere. In simpler words, a digital sphere is the set of integer points lying closest to the real sphere. In the adjacent figure, the centers of voxels actually constitute the set of 3D integer points corresponding to a digital sphere of radius 50. Since the solution lies in the integer domain, the challenge of the problem is in designing a sphere-generation algorithm using only integer operations, which will outweigh the performance of other algorithms based on approximation techniques, as shown recently in [3]. Hence, our scope of research in 3D digital geometry includes the following:



Digital sphere of radius 50 generated by our newly invented number-theoretic algorithm, which uses only integer operations.

1. Generation and analysis of digital sphere in 3D space.
2. Extension of number-theoretic interpretation to *digital hypersphere* in higher dimensional space.
3. Finding *digital sphericity* of a given set of integer points in 3D and higher dimensional space, which is a reverse problem and more difficult for applicability of number theory.
4. Generation of *surfaces of revolution* using number-theoretic properties.
5. Using the surfaces of revolution for computer graphics application.
6. Synthesis of other 3D digital non-polyhedral objects, e.g., ellipsoid, torus, etc.
7. Characterization of digital surfaces and applications to 3D imaging.

Very recently, we have succeeded in designing the algorithm to generate digital sphere using only integer operations. Such a number-theoretic approach can also be extended to generate hyper-spheres in digital space, which is our next target. Further, we would also explore the possibility of applying such number-theoretic techniques for analysis, characterization, recognition, and segmentation of other 3D surfaces, such as surfaces of revolution. Practicalities pertaining to testing with real-world data will also be addressed in our scope of research.

Sourya Bhattacharyya
Email: sourya.bhatta@cse.iitkgp.ernet.in
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 Bioinformatics Algorithms. His research interest is in analyzing genome sequences during phylogenetic evolution, and designing genome sequence reconstruction methods to generate ancestral genome ordering with respect to such phylogenetic evolution.*

Supervisor: Prof. Jayanta Mukhopadhyay

Computational analysis on phylogeny and ancestral genome ordering

Phylogenetic analysis helps to understand the evolutionary relationships between 'taxa' (entities such as genes, populations, species, etc.). It uses different protein or DNA sequences from various species as inputs, and generates the evolution history in either rooted or unrooted tree formats. Approaches such as: 1) Distance based clustering (such as UPGMA or Neighbor-Joining), 2) Distance optimality criterion (methods of minimum evolution or least square), and 3) Character based optimality criterion (Maximum parsimony or maximum likelihood), are employed to reconstruct the species tree which exhibits the evolutionary relationships between different species. However, analyzing the evolution in terms of genome sequences, which can be within one species or between species, is much more essential from a bio-medical research point of view. Genome mutations in abrupt large scale manner can be indicative of virus attack, disease or certain abnormal phenomenon. As a result, current research targets to construct a gene tree from input genome sequences, possibly with the help of a given species tree [1]. Due to availability of large genome sequences as standard datasets, such single or multi-species genome sequences can be compared to estimate the ancestral genome ordering, and the evolution taken place.

Genome sequences can be quite large or can be broken to the units of 'synteny blocks' (also termed as 'conserved segments') for individual processing [1]. Genome ordering refers to the signed permutations where each integer corresponds to a unique gene/marker and the sign corresponds to its orientation (strand) [2]. Individual genomes of same or different species are

analyzed in the context of genome rearrangement - that is, alteration of genome orders along different species or even within the same species [2]. Genome evolutionary operations include insertion, deletion, inversion, translocation, tandem duplication, segmental duplication, fusion, fission, etc [1]. Given the ordering of different gene sequences (uni-chromosome or multi-chromosome) from same or different species, the objective is to find mutual adjacencies of those sequences to infer the genome evolution. Such a problem requires extensive computation and approximate algorithms to model the diversity of the input species and corresponding genome sequences.

Considering the input genome sequences as the leaves of a rooted gene tree, the objective is to determine the root of the genome tree indicating the ancestral genome ordering. Intermediate nodes of the tree signify the evolutionary events to transform the ancestral genome to the input genomes (placed as the leaves). However, even for a single species, finding the optimal set of evolutionary operations and corresponding ancestral genome order is NP-hard problem [2]. As a result of approximation, initially some approaches [2, 3] fixed the genome size and analyzed only the genome rearrangement operations (excluding insertion, deletion, and duplication). Current approaches include insertion, duplication and loss (deletion) events. They approximate the evolutionary distance between pairwise genomes [4], and try to reconstruct ancestral genome order, incorporating both rearrangement, duplication and deletion operations [1, 5]. Still, there is a considerable gap in the theory of understanding the evolutionary process, and there is enough scope of improving the results on the formation of the phylogenetic trees. Proposed study is motivated towards that direction.

References

[1] Ma J., Ratan A., Raney B. J., Suh B. B., Zhang L., Miller W., and HausslerD., “DUPCAR: Reconstructing Contiguous Ancestral Regions with Duplications. Journal Of Computational Biology, 15(8):1007–1027, 2008.

[2] Bourque1 G., and Pevzner P. A. Genome-Scale Evolution: Reconstructing Gene Orders in the Ancestral Species. Genome Res, 12(1):26–36, 2002.

[3] Zhang Y., Hu F. and Tang J. A mixture framework for inferring ancestral gene orders. BMC Genomics, 13(Suppl 1:S7), 2012.

[4] Lin Y., Rajan V., Swenson K. M., and Moret B. M. Estimating true evolutionary distances under rearrangements, duplications, and losses. BMC Bioinformatics, 11(Suppl 1:S54), 2010.

[5] Vinar T., Brejova' B., Song G., and Siepel A. Reconstructing histories of complex gene clusters on a phylogeny. J Comput Biol, 17(9):1267–1279, 2010.

Moumita Saha
Email: moumitasaha2012@gmail.com
Joined the department in: July, 2012

Moumita Saha *received a B.Tech degree in Computer Science and Engineering from Meghnad Saha Institute of Technology, Kolkata in 2010, and an M.E. degree in Computer Science and Engineering from Bengal Engineering and Science University, Shibpur, Howrah in 2012. Since July 2012, she has been a research scholar in the department of Computer Science & Engineering in IIT Kharagpur. Her primary research interest are pattern recognition and knowledge mining.*

Supervisor: Prof. Pabitra Mitra

Multi-View Clustering for Richly Structured Data

Clustering is an approach of partitioning the data objects into groups such that the similarity between the data objects of same cluster is most and that between the objects of different clusters is least. Thus, it is a procedure of data exploration which is an efficient way of searching for patterns in the data. It is the most common form of unsupervised learning which is utilized to determine intrinsic grouping in a set of unlabeled data.

A challenging problem in data mining is mining richly structured data sets, where the objects are linked in some way. The richly structured data set found to be available in multiple representations or views, i.e. the same class of entities can be observed or modeled from various perspectives leading to multiple-view representation. Multi-view learning is an important approach to effectively explore and exploit the information from multiple-view data for the purpose of improving the learning performance. Multi-view algorithms deals with each view of the data independently and then merge the solutions to obtain a complete, robust pattern as compared to its single-view.

The work has application in the field of text mining, information retrieval, market segmentation, sensor surveillance, bioinformatics, medical diagnosis, building of smart cities etc.

The broad goal is set for research on multi-view clustering on richly structured data. Traditional clustering methods deal with single view of data. However, at present the relational data are

much structured and complex. They can be analyzed from different perspective. We can obtain a better consequence if we analyze them from all possible perspective and combine the different consequences. Multi-view clustering performs the task, it execute the clustering job taking suitable similarity measure independently for different views of data and finally output the clusters which are more logical and more rich information-content.

We will be utilizing graph based approach. We will focus on heterogeneous graph coupling in order to analyze similarity measure for the purpose of clustering. Each object should be grouped in multiple clusters, representing different perspective of data. Each solution provides additional knowledge and thus results in enhanced extraction of knowledge.

Priyanka Sinha
Email: priyanka@cse.iitkgp.ernet.in
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.*

Supervisor: 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 companywide social media are suffering from any technical challenge and redirect them to possible solutions.

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

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

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. We aim 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.

Sandipan Sikdar
Email: sandipansikdar@cse.iitkgp.ernet.in
Joined the department in: December 2012

Sandipan Sikdar *received a B.Tech. degree in Computer Science and Engineering from Institute of Engineering and Management, Kolkata in 2012. Since December 2012, he has been a research scholar as well as Senior Research Fellow in the department of Computer Science & Engineering in IIT Kharagpur. His research interests are in Time Varying Networks.*

Supervisors: Prof. Animesh Mukherjee and Prof. Niloy Ganguly

Time varying networks

Complex networks have been a hot topic of research since the last decade. Almost every real interacting system (e.g., World Wide Web, the Internet, biological pathways, online and offline social relationships) can be represented as a complex network. That their degree distribution follows power law and that they have a tendency to form clusters have been identified. Apart from these many other properties (like small-world effect) have been discovered and numerous generative models have also been proposed to demonstrate the emergence of these properties. However, the underlying assumption in almost all these studies has been that the network is static, i.e., the statistical properties of the topology remain the same. Only recently, there has been consensus in the research community that real networks have nodes/edges dynamically entering and leaving the system thus making the topological properties dependent on time. Although properties like degree distribution, clustering coefficient etc. quite succinctly allow us to visualize the structure of a static network, the same is not true for a time-varying network [1[2][3]. In fact, there is no known quantitative measure suggested in the literature that explains the behavior of time-varying networks .In this research we identify one such property that, we believe, can significantly portray the topology of such time-varying graphs – the precise autocorrelation of the same graph at different time-points. We believe, that this time correlation for real systems is far from being random and therefore should be able to properly signal the characteristics of real time-varying graphs. We plan to quantify this autocorrelation using suitable quantitative measures adopted from the fields of data-mining, image processing, signal

processing where the idea of autocorrelation is heavily used. We further plan to deeply investigate how different changes in the network can affect the autocorrelation and finally build up a model of time-varying graphs that is able to predict the autocorrelation patterns observed in real graphs. This should then be able to indicate the natural mechanism that is instrumental in the "time-dependent variation" of the graph structure.

Further, as an application, we plan to investigate the time-varying aspect of citation networks [4]. In particular, the objective is to show how the temporal change in the citation patterns affects shift in research focus within a scientific domain, for example, the Computer Sciences. A central issue here is to define the authoritativeness [5] of a field (e.g., fields like algorithms, computer networks, artificial intelligence, databases, machine learning etc.) within the domain in terms of the number of citations received by the research papers in that particular field. An early result indicates that a field that is ranked second in terms of its authoritativeness emerges as the leader in near future. In addition, we also wish to investigate the effect of geographic variations on citation patterns and whether that has some influence on the shift of research focus.

References:

[1] Peter Holme and Jari Saramäki, Temporal Networks, arXiv:1108.1780 [nlin.AO], 16 Dec 2011

[2] Michele Starnini, Andrea Baronchelli, Alain Barrat and Romualdo Pastor-Satorras, Random walks on temporal networks ,PHYSICAL REVIEW E 85, 056115 (2012)

[3] N. Perra1, B. Gonçalves, R. Pastor-Satorras and A. Vespignani, Activity driven modeling of time varying networks, Scientific Reports, June 2012.

[4] E. Garfield, I. H. Sher, and R. J. Torpie. The Use of Citation Data in Writing the History of Science. Institute for Scientific Information Inc., 1984.

[5] R. Guns and R. Rousseau. Real and rational variants of the h-index and the g-index. Journal of Informetrics, 3(1):64–71, 2009.

MS Scholars

RitwikaGhose
Email: ritwika.ghose@gmail.com
Joined the department in: September 2009

RitwikaGhose*received a B.E. degree in Information Technology from West Bengal Institute of Technology, Kolkata in 2009. Since September 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 Human Computer Interaction, Natural Interface Design and Assistive Technologies.*

Supervisor: Prof. Anupam Basu

Web Browsing System for the Blind People

With the advancements in computers and technology, access to electronic information by blind people has been easier over the years. Printed Braille documents and the aid of human readers have been replaced by software agents like screen readers and tactile devices. However, since most of the information available in the World Wide Web is designed for the sighted people, the blind community faces a number of challenges in accessing the same materials. The main focus of this research is to analyze the existing problems of web browsing by the blind people and to develop an enhanced browser system to circumvent the identified obstacles.

There are three main aspects of web browsing- operations on the web browser interface, browsing through the contents of a web page, and navigating through different web pages. The web browser interface accepts user query, performs the corresponding action and presents the output of the action to the user. A web page that is presented to the user contains information in various forms, plain text, hyperlinks, lists, image, etc. The users can then locate and read their desired areas in that page. The third aspect is navigation, which involves moving through different web pages either by clicking hyperlinks in the current page, or giving the URL link directly to the browser.

The main mode of accessing information from the Web for the blind users is through speech. With the advent of text-to-speech systems, use of screen readers has been popular among the blind community. The screen is read out from top-left to bottom-right by a screen reader; the layout, structure, colors and other visual features are lost in this representation. The browser interface elements are usually organized in menus and icons; hence sequential reading of the options by a screen reader increases the access time in locating the desired function. An alternate method of accessing the functions is via shortcut keys. However, it is particularly difficult for novice blind users who are not accustomed with either the keys in the keyboard, or the key combinations for the particular operations. In case of web pages, often the flow of information as depicted by the visual layout is disrupted, and may produce disjointed feedback. The presentation of information in web pages mostly focuses on the design and structures, catering to the interests of the sighted users. However, visual representations like separators, color differences between sections, decorations etc. are not only lost on a blind user but also pose considerable challenges for them.Poorly designed pages with unlabeled form items, or pictures with no meaningful alternate texts, inaccessible scripts, etc. add to the confusion in screen reader feedback. A sighted user may easily skip irrelevant information and locate their area of interest, whereas a blind user has to move sequentially through all the segments to determine its relevance. All these factors necessitate the presentation of web content to be different for blind users from the original presentation which is primarily meant for sighted users.

In order to address the above issues, alternate presentation schemes for both, browser interface and web pages have been proposed in this research. Apart from the standard methods of accessing a function in the browser interface, the enhanced browser system have been integrated with an Automatic Speech Recognition system, to accept voice commands corresponding to the browser functions. In order to further aid novice users who are not accustomed with the available options, a reduced set of browser operations is anticipated and presented to the user at specific points of time during browsing. An alternate presentation of web pages has been proposed in this research in order to produce a suitable one-dimensional output of the page content to be inputted to the screen readers. In order to reorganize the page, the page structure and the underlying elements have been analyzed. Next, a categorization algorithm has been applied to the pages in order to identify the type of page it represents. Finally, using the above results, a suitable linear order among the different elements of the page is obtained and presented to the user.

Binanda Sengupta
Email: binanda.sengupta@cse.iitkgp.ernet.in
Joined the department in: July 2010

Binanda Sengupta *received his B.E. degree in Computer Science and Engineering from Jadavpur University, Kolkata in 2007. From 2007 till 2010, he worked in Tata Consultancy Services Limited, Kolkata, as an Assistant Systems Engineer. Since July 2010, he has been an MS student in the department of Computer Science & Engineering in IIT Kharagpur. His research interest includes Cryptography and Computational Number Theory.*

Supervisor: Prof. Abhijit Das

Parallelization of Different Sieving Techniques

Different sieving techniques are used extensively in solving number-theoretic hard problems like Integer Factorization Problem and Discrete Logarithm Problem. These techniques are incorporated to make the running time sub-exponential (though super-polynomial). We are trying to implement these techniques efficiently and parallelize them in order to reduce the running time.

Partha De
Email: partha.de@cse.iitkgp.ernet.in
Joined the department in: July2010

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 data path 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 AES 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 processor. It’s easy to implement crypto 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 crypto processor implementation, a dedicated crypto block of the crypto 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 AES processor. My next objective is to fabricate AES processor using UMC 180nm technology and also examine the power characteristics.

Rajdeep Mukherjee
Email: rajdeep.mukherjee@cse.iitkgp.ernet.in
Joined the department in: July 2010

Rajdeep Mukherjee *received his B.Sc. and B.Tech. degree in Computer Science from University of Calcutta, Kolkata in 2007 and 2010 respectively. Since July 2010, he has been a MS (by research) student in the department of Computer Science & Engineering at IIT Kharagpur and he also works as a Research Consultant in a project entitled "Power Intent Verification" from Synopsys, Inc. since July 2010. His research interests are in the areas of Formal Verification, Software Verification, Low-power Design, EDA, CAD and High-level Synthesis.*

Supervisor: Prof. Pallab Dasgupta and Prof. Ajit Pal

SYNTHESIS AND VERIFICATION OF POWER MANAGED DIGITAL INTEGRATED CIRCUITS

Low power design is important in today's deep ASIC submicron era for different reasons, which include increased device temperature, rise in failure rate, high cooling and packaging costs, prolonged battery life and environmental impact. Several advanced design techniques have been adopted for the implementation of low power systems. All these techniques require additional hardware and software support for proper management of system power. Typically, the power management can be done at *system level*, *architecture*, *gate*, *circuit* and the transistor level. All these design levels use some form of fine-grain or coarse-grain strategies of managing power.

Effective on-chip power management has become one of the primary goals in the design of large scale digital integrated circuits. There exists a wide arsenal of power management techniques, including techniques for decomposing a design into several power domains, managing dynamic power such as clock gating, voltage and frequency scaling, and managing leakage power such as power gating and adaptive body-biasing. In a complex architecture, a combination of these strategies may be used for better power management. The additional design complexity arising due to incorporating power managed circuitry and techniques may lead to design errors and new bugs. Thus, it is imperative to verify whether the design operates correctly in each power domains and the sequencing of these power state transitioning in individual domains are correctly implemented. Verification of architectural power management strategies are also of

primary concern in today's complex electronic systems. Verification guarantees the correctness and completeness of a system design with respect to the design requirements which are specified by formal properties using temporal logics. Specifically this research addresses the following broad objectives:

1. **Multi-objective low-power CDFG Scheduling using fine-grained DVS Architecture:** To build a multi-objective low-power high-level synthesis systems using fine-grained DVS enabled resources under different constraints. Given an input behavioral description captured using control data-flow graph, constraints like latency bound, and an optional area or power budget, our objective is to generate pareto-optimal schedule of <area, power>tuples satisfying these constraints using fine-grained DVS enabled functional modules.

2. **Power Aware Scheduling during high-level synthesis stage using DVS Architecture in Distributed Framework:** We propose a branch-and-bound based low-power scheduling algorithm in distributed environment under strict and relaxed timing constraints.

3. **Power and Temperature aware Scheduling and Binding solutions during behavioral synthesis stage using fine-grained DVS Architecture:** Develop an integrated framework for fine-grained power management and thermal management during high-level synthesis stage. In order to alleviate hotspots, the multi-objective algorithm tries to minimize the peak switching activity SW_{peak} of the modules involved in the synthesis process.

4. **Hardware/Software Co-verification of Power Management Strategies in Embedded Controllers:** To develop a formal verification methodology for hardware/software co-verification of power management strategies in complex embedded power controller. One of the primary challenges in verifying such power management architectures stems from the mixed implementation of such strategies, where the local power controllers are in hardware and the global power management is implemented in software/firmware.

5. **Model Checking of Global Power Management Strategies in Software with Temporal Logic Properties:** To verify the global power management strategies in Software with Linear Temporal Logic (LTL) properties using bounded model checking approach and a comparative study of the same is done using SATABS and CBMC. The temporal properties are translated in to assertions and instrumented in the software controller for model checking in CEGAR loop.

6. **Bounded Model Checking based Verification of Hardware/Software Implementation of Power Management Strategies using HW-CBMC:** To perform bounded model checking based Verification of Hardware/Software implementation of Power Management Strategies using HW-CBMC and scalability of the approach using HW-CBMC is addressed. The method easily scales up to several hundred power domains. The software program is treated as a transition relation and the program is unwound up to a bound of k, where the value of k must be greater than or equal to maximum depth of the architectural property. Our model works in a way that the software controller drives these hardware controllers and this is done in HW-CBMC tool by using next_timeframe() function which ensures that the verilog modules make a transition once this function is called inside the software controller.

Tamal Sen
Email: tml.cse@gmail.com
Joined the department in: December, 2010

Tamal Sen *received his BTech (2008) degree in Computer Science and Engineering from Jalpaiguri Govt. Engg. College. From Feb'09 to Nov'10 he worked in Cognizant Tech. Solutions, Kolkata. Since Dec'10, he has been a MS scholar in the department of Computer Science & Engineering in IIT Kharagpur. His research interests are in the areas of program analysis and effort minimization in software testing.*

Supervisor: Prof. Rajib Mall

Regression Test Selection for Component-Based Software

A component is a cohesive group of reusable services that have been collated into an executable unit. Components are developed independently, available off-the-shelf and integrated into a component based system by the application developers. Component-based development has found rapid acceptance by software developers since it is realized that reuse of components helps lower the development cost and speed up the development process.

Components can be written in different programming languages and may be distributed across different platforms. Source code is not usually disclosed to the application developers. Components can have two different types of operations: provided and required. Provided operations are those which have been implemented in the component and they can be invoked from the outside. In the other hand, concrete implementation of the required operations is left to the users of the component. The provided and required operations are published through the interfaces called required interfaces and provided interfaces respectively. Interfaces are generally defined using an interface definition language (IDL). The application developers (the users of the components) make use of interface definitions of the components to develop an application.

A major difficulty in component based development is that unavailability of source code makes software engineering tasks difficult to carry out. In addition to the development activities, testing activities like coverage analysis, regression test selection etc. turn out to be even more challenging.

Regression testing is carried out after every code modification to ensure that the unmodified functionalities continue to work satisfactorily. Regression test selection (RTS) is the process of selecting a subset of system test cases which can effectively find all errors that might get induced in the unmodified parts.

In case of component-based systems, new versions of the components are released very frequently. In this context, analyzing change impact and selecting a safe subset of the system test cases for regression testing involve high overhead, thereby pose significant challenge.

For component-based software, applying traditional RTS techniques is difficult because application developers do not have the source code for analyzing change impact; neither can they obtain coverage data of the test suite through code instrumentation. It may be unrealistic to expect component vendors to provide that information due to obvious reasons. To facilitate regression testing, component vendors either need to provide Built-In-Test interfaces or after each modification, they are expected to provide the change information in terms of some published elements (such as method signature, pre/post conditions etc.).

The simplest form of change information can be a collection of affected methods which could be published after every modification to a component. Techniques for identifying affected methods can be simply choosing those methods which have been modified or those that directly or indirectly call a modified method. But errors can exist in the unmodified parts of the code due to its dependencies on the actually modified parts. It is suggested that analysis of control and data dependence relationships is necessary for detecting many types of code-based faults. Hence, the methods which may execute some of those indirectly affected statements need to be included in the change information in order to perform a better regression testing.

In contrast to what is implicitly assumed by many existing techniques, invoking an affected method does not ensure that all affected statements inside that method will be executed. It can be argued that, since most components have non-trivial state models, some statements inside a method may remain unreachable in some states, even if the method is invoked in all possible ways. Pure dependence based techniques choose test cases which invoke one or more component methods which have been found affected by dependence analysis. Some test cases, chosen by pure dependence based technique, can be redundant if they invoke affected methods in a state such that no affected statements are reachable. We propose an RTS technique for component based software which includes an enhanced mode of publishing change information by statically analyzing the source code of a component. The approach can reduce regression testing effort significantly by reducing the number of regression cases.

Indrasish Saha
Email: indrasish88@gmail.com
Joined the department in: July 2011

Indrasish Saha *received a B.E. degree in Information Technology from Jadavpur University , 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 Hardware Security and Machine Learning.*

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

Model Building Attacks on Physically Uncloneable Functions

A Physical Random Function or Physical Unclonable Function(PUF) is a function that is based on a physical system that is easy to evaluate (using the physical system) and its output looks like a random function which is unpredictable even for an attacker having physical access.In the context of intrinsic physical properties of integrated circuits, Physically Unclonable Functions (PUFs) can be usedto complement classical cryptographic constructions, and to enhance the security of cryptographic devices. PUFs have recently been proposed for various applications, including anticounterfeiting schemes, key generation algorithms, and in the design of block ciphers.

Numerical modeling attacks on PUFs presume that an adversary Eve has collected a subset of all Challenge-Response pairs of the PUF, and tries to derive a numerical model from this data, i.e. a computer algorithm which correctly predicts the PUF's responses to arbitrary challenges with high probability. If successful, this breaks the security of the PUF and of any protocols built on it. We have collected Challenge-Response pairs for Arbiter and Ring Oscillator based PUFs and propose to build genetic programming techniques for such modeling attacks.

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

Suman Kalyan Maity *has received a B.Tech. degree in Computer Science & Engineering from National Institute of Technology, Durgapur 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 Complex Systems and Language Dynamics.*

Supervisor: Prof. Animesh Mukherjee

Opinion formation in social networks: The case of the naming game

Social phenomena are inherently complex. The detailed behavior of such social systems that result from the complex physiological and psychological processes are still largely unknown. One such fundamental phenomenon in social dynamics is the transition from disordered to ordered/fragmented state like the spontaneous formation of a common language/communication scheme or the emergence of consensus or agreement on a particular issue. This agreement/consensus is one of the most important aspects of social group dynamics. We live in a world where everyday life presents 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.

There has been a lot of research on opinion dynamics and a wide variety of opinion formation models exist in literature. In this report, we shall focus on a popular model of consensus dynamics -- the "Naming Game". The evolution of the system in this model takes place through the usual local pairwise interactions among artificial agents that necessarily capture the generic and essential features of an agreement process. This model was expressly conceived to explore the role of self-organization in the evolution of languages and has acquired a paradigmatic role in semiotic dynamics that studies evolution of languages through invention of new words, grammatical constructions and more specifically, through adoption of new meaning for different

words. NG finds wide applications in various fields ranging from artificial sensor network as a leader election model to the social media as an opinion formation model.

The minimal naming game consists of a population of N agents observing a single object in the environment (may be a discussion on a particular topic) and opining for that by means of communication with one another through pairwise interactions, in order to reach a global agreement. The agents have at their disposal an internal inventory, in which they can store an unlimited number of different words or opinions. At the beginning, all the individuals have empty inventories. At each time step, the dynamics consists of a pairwise interaction between randomly chosen individuals. The chosen individuals can take part in the interaction as a "speaker" or as a "hearer." The speaker voices to the hearer a possible opinion for the object under consideration; if the speaker does not have one, i.e., his inventory is empty, he invents an opinion□. In case where he already has many opinions stored in his inventory, he chooses one of them randomly. The hearer's move is deterministic: if she possesses the opinion pronounced by the speaker, the interaction is a "success", and in this case both speaker and hearer retain that opinion as the right one, removing all other competing opinions/words from their inventories; otherwise, the new opinion is included in the inventory of the hearer, without any cancellation of opinions in which case the interaction is termed as a "failure". The game is played on a fully connected network, i.e., every agent can, in principle, communicate with every other agents, and makes the following assumption. It is assumed that there can be potentially huge number of opinions for a particular topic so that the probability that two players will ever invent the same opinion at two different times is practically negligible and that the environment consists of a single topic of discussion.

Opinion formation on time-varying social network

We consider the naming game dynamics on two different types of time-varying data; one varying on a day-to-day basis while another varying over very short intervals of time (20 seconds). In the first case, we observe that networks with strong community structures delay the convergence due to co-existence of competing and long-lasting clusters of opinions. In the second case, the games are played in perfect synchronization with the time-evolution of the network. In this case, we observe that the global observables are markedly different from the case where the games are played on the static (and composite) version of the same network as well as from the traditional results reported in the literature.

Effect of dominance on the emergence of agreement on social network

This work focuses on the impact of dominance of certain opinions over others in pursuit of faster agreement on social networks. We propose two models to incorporate dominance of
the opinions. We observe that both these models lead to faster agreement among the agents on an opinion as compared to the minimal naming game reported in the literature. We perform extensive simulations on computer-generated networks as well as on a real online social network (Facebook) and in both cases the dominance based models converge significantly faster than the minimal model.

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: Dr. DebdeepMukhopadhyay

Towards multivariate DPA using a formal approach

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 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 methods 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) methods requires detail knowledge of the 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 (which are the more likely scenarioes in future) 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.

Arnab Dhar
Email: arnab832007@gmail.com
Joined the department in: January 2012

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.

Debapriya Basu Roy
Email: dbroy24@gmail.com
Joined the department in: July 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: Dr. Debdeep Mukhopadhyay.

Accelerating Finite Field Operations & Side Channel Analysis of Cryptographic Algorithms on FPGAs

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 paper 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. Next, we are going to discuss about side channel analysis of key encapsulation algorithm PSEC-KEM which operates on elliptic curves.

PSEC-KEM is a provably secure key encapsulation mechanism. It is used to realize key agreement schemes. By the term ‘Side Channel’, we mean any information which is gained from the hardware implementation of the cryptographic algorithm. For this work, we have focused on ‘power’. Successful power attack on a specific cryptographic algorithm requires proper

understanding of the vulnerabilities of an implementation of that algorithm and developing attackstrategies exploiting those vulnerabilities. However, successful attack also depends uponcorrect acquisition of the power traces. Hence developing a proper setup which will enableus to collect power traces accurately is of primary importance. Experiments have been carried out on SASEBO (Side Channel Evaluation Board). Power traces are acquired from a mixed signal oscilloscope. PSEC-KEM is implemented in four different fields- 1) binary random curve 2) Koblitz curve 3) prime non-endomorphic curve 4) prime endomorphic curve. Side channel analysis for PSEC-KEM in different fields is presented in this project. Successful attack strategies for each of the implementation is also have been implemented. Next, we are going to discuss about the frequency dependence of SCA resistance in case of AES.

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.

Souvik Kolay
Email: souvik1809@gmail.com
Joined the department in: July, 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.*

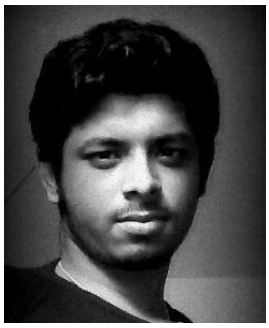
Supervisor: Dr. Debdeep Mukhopadhyay.

Design of Dedicated Instruction for lightweight cryptography and Design and Analysis of Lightweight Block Cipher on FPGAs

Security has been one of the most important issues for computer networks. With the growing demand of applications, there has been significant impetus on the design of less costly, high performance solutions for cryptographic algorithms. These cryptographic algorithms comprise of complex mathematical operations, making such designs increasingly challenging. Software implementations of ciphers on general purpose processors are flexible, but slow in performance. On the other hand hardware implementations of ciphers have a better performance, but are costly and lack in flexibility and programmability. In order to suitably trade off these two ends of the spectrum, application specific processors have emerged for cryptography. However a very important step is in the identification of the instruction set and providing suitable support for the same. Thus a superior Instruction Set Architecture (ISA) would lead to better result both in terms of speed and cost, which is affected by the resource utilization required to support the instruction. In this project, we have shown that bit-permutation is one of those costly operations, which can be accelerated by providing dedicated instructions. Further, we have proposed, an instruction for bit-permutation, named *PERMS*, which is capable of performing any n bit arbitrary permutations, using (log n) instructions. The hardware implementation costs of

*PERMS*shows that it is lightweight than any existing bit-permutation instructions, which make it suitable for lightweight cryptography. We have also checked the performance of *PERMS*, by adding this instruction with standard ISA and the result shows that up to 50% improvement on performance can be achieved on the standard cryptographic algorithms.

Pervasive computing or ubiquitous computing is the growing trend towards embedding microprocessors in everyday objects so that they can communicate information. Pervasive devices, like RFID, possess very limited resources in terms of memory, computing power and battery supply, but many applications running on these devices will contain sensitive information and there lies the need of cryptographic systems to ensure its security. This area of cryptography which deals with the design, analysis and implementation of cryptographic algorithms for devices with extremely constrained resources is formally termed as lightweight cryptography. In the second research project, our object is to design a Lightweight Block Cipher, which will be light enough for implementing in FPGA and at the same time will provide the desirable security and good throughput. We have studied that design strategies for lightweight ciphers on FPGAs, are significantly distinct from ASICs. For this reason, an existing lightweight cipher for ASIC may not be equally lightweight, while implementing on FPGA. Further, we have found some strategies to design lightweight block cipher for FPGAs. Following those strategies, we have design a 64-bit cipher, named *Khudra*, which supports 80 bits key. For the compact implementation, it requires only 138 slice and for better throughput implementation, it requires 165 slices. Further we have also analyzed the security of *Khudra*, against the standard cryptanalysis, and found it to be secured against the Linear Cryptanalysis, Differential Cryptanalysis, Liner-Differential Cryptanalysis, Impossible Differential Cryptanalysis, Algebraic Attack, Boomerang Attack. Slide Attack and Relative Key Attack. Finally, we have compared the implementation result of *Khudra*, with two best existing lightweight block ciphers for ASIC: *Present* and *Piccolo*, and the comparison shows that *Khudra* takes less slices and produces better throughput than any of these two ciphers.



Parnab Kumar Chanda
Email: parnab.2007@gmail.com
Joined the department in: January 2012

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 July2011, 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 can be seen into 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 generation 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.

Ayan Palchaudhuri
Email: ayan@cse.iitkgp.ernet.in
Joined the department in: February 2011

Ayan Palchaudhuri *received a B.Tech. degree in Electronics and Communication Engineering from West Bengal University of 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 VLSI and Reversible Watermarking of Digital Images.*

Supervisor: Prof. Rajat Subhra Chakraborty

FPGA based Hardware Design for Real-time Reversible Watermarking of Digital Images

Digital watermarking has been widely used to protect the copyright of digital images. In order to strengthen the intellectual right of a digital image, a trademark of the owner could be selected as a watermark and embedded into the protected image. Then the watermarked image could be published and the owner can prove the ownership of a suspected image by retrieving the watermark from the watermarked image. For some critical applications such as the law enforcement , medical and military image system , it is crucial to restore the original image without any distortions. The watermarking techniques satisfying these requirements are referred to as 'reversible watermarking'. Reversible watermarking is designed so that it can be removed to completely restore the original image.

Watermarking implementations can be done in software or in hardware. Although it might be faster to implement an algorithm in software, there are a few compelling reasons for a move towards hardware implementation. A hardware watermarking solution is often more economical because adding the watermarking component takes up a small dedicated area of silicon. In software, implementation requires the addition of a dedicated processor such as a DSP core that occupies considerably more area, consumes significantly more power, and may still not perform adequately fast.

Hardware implementations of watermarking can be implemented in Application Specific Integrated Circuits (ASICs) or in Field Programmable Gate Arrays (FPGAs). Most of the current hardware implementations have been done for ASIC designs. Recent advances in FPGA technology, such as 90nm process devices, higher gate densities, better interconnect architectures, reduction in power consumption, multiple I/O formats and embedded optimized logic, have allowed for applications that were previously intended for ASICs to be implemented in FPGA devices, with the added value of a lower FPGA cost when compared to an ASIC.

Designing efficient architectures using an FPGA platform is not trivial as the designer has to optimally exploit dedicated routing resources and fast logic gates like multiplexers available within FPGAs to reduce the critical path of the most common arithmetic and logic operations executed in digital applications. Performances can also be significantly influenced by the computational capability offered by the Look-Up-Tables(LUTs) typically available within FPGAs as certain LUTs are dynamically reconfigurable and some even offer a second output for implementation of any 5-input 2-output function which otherwise would have required 2 LUTs for realization. Insertion of latches at appropriate locations leads to pipelining which increases the speed and throughput of the architecture. As the resources available on FPGA platforms are in plenty, we can always aim for higher speed and better performance with a reasonable area overhead.

Shamit Ghosh
Email: shamit.ghosh@cse.iitkgp.ernet.in
Joined the department in: May, 2012

Shamit Ghosh *received his B.E. degree in Computer Science & Engineering from Jadavpur University, Kolkata in 2011. He joined as MS scholar in the department of Computer Science & Engineering in IIT Kharagpur in June 2012. His research interests lie in the areas of Cryptography.*

Supervisor: Prof. Dipanwita Roy Chowdhury.

CA based Side Channel Prevention of Leakage Squeezing, Cryptography

I had worked on a project on "Encryption in Compressed Domain" which was on real time audio transmission securely using GRAIN stream cipher. Currently I am working on leakage squeezing of order two and its implementation using Cellular Automata (CA) for side channel prevention.

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

Abhrajit Sengupta*received his B.E. degree in Computer Science & Engineering from Jadavpur University, Kolkata in 2011. He joined as MS scholar in the department of Computer Science & Engineering in IIT Kharagpur in June 2012. His research interests lie in the areas of Cryptography.*

Supervisor: Prof. Dipanwita Roy Chowdhury

Design and Implementation of Code based Cryptographic Schemes

Currently I'm working on some practical key recovery attack on two variants of McEliece cryptosystem. Basically these schemes replaced Goppa codes with some highly structured codes to reduce the key size. Our idea is to exploit this underlying structure of the error correcting codes used in these variants. We are trying to formulate a set of equations from the structural nature of the codes, and by solving it we can break the scheme successfully.

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.

Swadhin Pradhan
Email: swadhin.pradhan@cse.iitkgp.ernet.in
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 specfic 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, location based services, and data analytics in physical space like super market.

Our Mentors:
Faculty of the Department

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

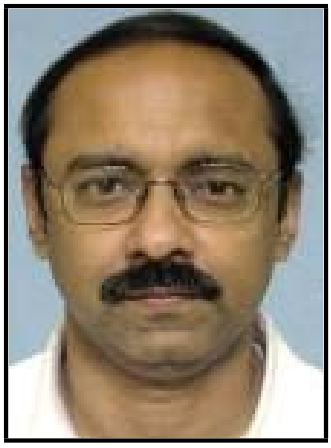
Research Interests: *Image and video processing, pattern recognition and multimedia system*

Jayanta Mukhopadhyay 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 transferred 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 was a Humboldt Research Fellow at the Technical University of Munich in Germany for one year in 2002. He also has 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 has published over 100 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. He is a fellow of the Indian National Academy of Engineering (INAE).

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

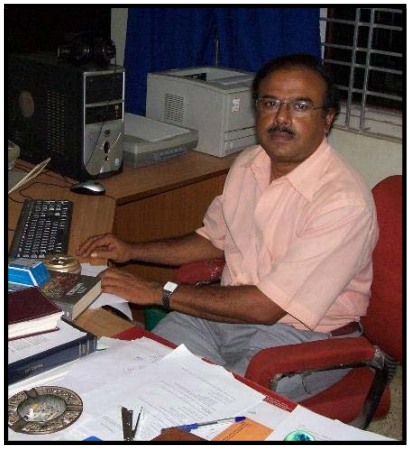


Arobinda Gupta

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.



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

Research Interests: *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.

Ajit Pal

Email: apal@cse.iitkgp.ernet.in

Research interest: *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 for 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 135 publications in reputed journals and conference proceedings and two books entitled `Microprocessors: Principles and Applications' published by TMH (1990) and `Microcontrollers: Principles and Applications' published by PHI (2011). He is the Fellow of the IETE, India and Senior Member of the IEEE, USA.

Abhijit Das

Email: abhij@cse.iitkgp.ernet.in

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

Abhijit Das is Assistant Professor, Department of Computer Science and Engineering, Indian Institute of Technology Kharagpur. He has held academic positions at the Indian Institute of Technology Kanpur and Ruhr-Universität Bochum, Germany. His research interests include arithmetic and algebraic computations with specific applications to cryptology.

Animesh Mukherjee

Email: animeshm@cse.iitkgp.ernet.in

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

Chittaranjan Mandal

Email: chitta@cse.iitkgp.ernet.in

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

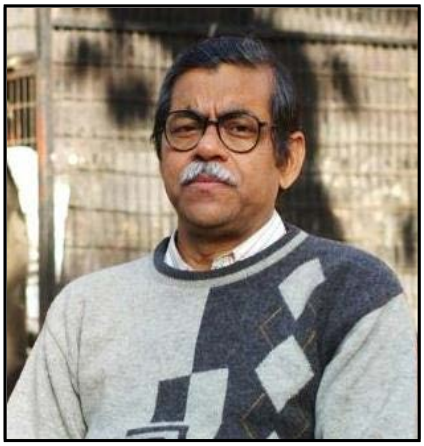
Chittaranjan Mandal received his Ph.D. degree from IIT, Kharagpur, India, in 1997. He is currently a Professor with the Department of Computer Science and Engineering and also the School of Information Technology, IIT, Kharagpur. Earlier he served as a Reader with Jadavpur University. His research interests 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 Interest: *Cryptography, Side Channel Analysis, VLSI of Cryptographic Algorithms, Cellular Automata*

Debdeep Mukhopadhyay is presently working as an Assistant Professor in the Computer Sc and Engg Dept from June 2009. Prior to this he worked as an Assistant Professor in the Dept of Computer Sc and Engg, IIT Madras. Debdeep obtained his BTech from the Dept of Electrical Engg, IIT Kharagpur in 2001. Subsequently he obtained his MS Degree in 2004 and PhD from the Dept of Computer Sc and Engg, IIT Kharagpur in 2007. He has authored about 10 Journal and 49 Conference papers and has served in the Program Committee and as Reviewers of several International Conferences and Journals. Debdeep has been awarded the Indian Semiconductor Association (ISA) TechnoInventor award for best PhD Thesis in 2008.



Dipankar Sarkar

Email: ds@cse.iitkgp.ernet.in

Research interest: *Formal Verification and Symbolic Reasoning*

D. Sarkar did his B.Tech., M.Tech. in Eletronics and Electrical Communication Engg. and PhD in Engineering from I.I.T., Kharagpur. He has served I.I.T., 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 Interest: *Theoretical computer science, compiler*

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 presently being 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.

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

Research Interests: *Peer-to-peer Networks, Complex Network Theory, Social Networks Modelling*

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

Partha Bhowmick

Email: pb@cse.iitkgp.ernet.in

Research areas: *Digital geometry, Shape analysis, Computer graphics.*

Partha Bhowmick graduated from the Indian Institute of Technology, Kharagpur, India, and received his master's and PhD degrees from the Indian Statistical Institute, Kolkata, India. He is currently working as an Assistant Professor in the department of Computer Science and Technology, Indian Institute of Technology, Kharagpur, India. His primary research interest is digital geometry, pertaining to algorithms in the digital paradigm and involving potential applications in computer graphics, low-level image processing, approximate pattern matching, shape analysis, GIS, and biometrics. He has published over 45 research papers in international journals, edited volumes, and refereed conference proceedings, and holds three US~patents.

Pallab Dasgupta

Email: pallab@cse.iitkgp.ernet.in

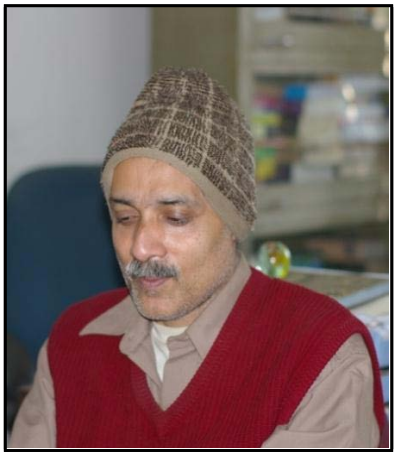
Research interest: *Formal Verification, Artificial Intelligence and VLSI.*

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.

Partha Pratim Chakrabarti
Email: ppchak@cse.iitkgp.ernet.in

Research Interests: *Artificial Intelligence, Algorithms for Design Automation in VLSI and Embedded Systems*

Partha P Chakrabarti is a Professor in the Department of Computer Science and Engineering at Indian Institute of Technology, Kharagpur. Currently he is also holding the post of Dean SRIC (Sponsored Research and Industrial Consultancy) and Head of the Advanced Technology Development Centre (ATDC) at IIT Kharagpur. 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. As Dean 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.

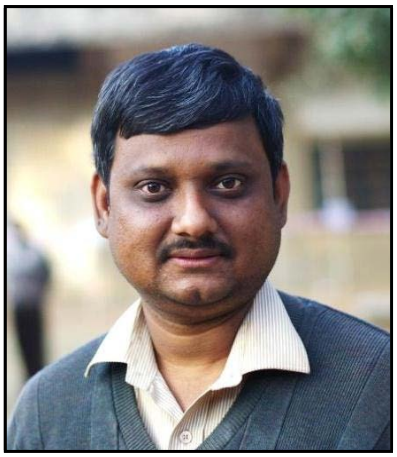


Partha Sarathi Dey

Email: psd@cse.iitkgp.ernet.in

Research Interest: *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



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.

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

Research Interests: *Object-oriented analysis and design, software engineering, image rocessing, digital geometry, electronic design automation*

Rajat Subhra Chakraborty
Email: pabitra@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 implementation of cryptographic algorithms and digital-watermarking.

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

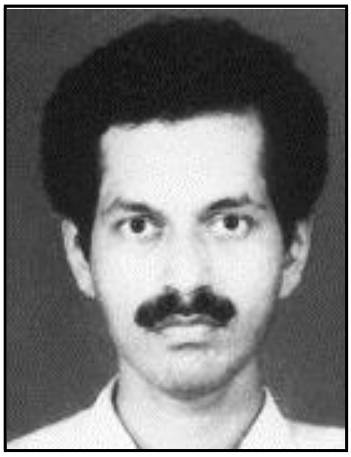
Research Interest: *Programming Languages & Software Engineering, Embedded & Multimedia system, Evolutionary Computing*

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. 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.



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

Research Interest: *Design and analysis of computer algorithms, particularly in the domain of geometry and graph theory*

Sudebkumar Prasant Pal has research interests in the design and analysis of computer algorithms, particularly in the domain of geometry and graph theory. His current research contributions and interests are in the areas of (i) visibility problems in polygons, (ii) hypergraph coding and coloring, (iii) combinatorial aspects of multipartite quantum entangled states, and (iv) entanglement-assisted quantum protocols defined across a network of remote sites. In the area of computational geometry, he has contributed results on weak and convex visibility, 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. In recent years, he has worked on (i) combinatorial characterizations of LOCC incomparable ensembles of multipartite quantum entangled states, and (ii) purely caching based video feeds as opposed to streaming, for scalable video service by introducing the notion of virtual caching in internet proxies. He has held positions such as (i) Convenor, Advisory Committee for the Centre for Theoretical Studies, I.I.T., 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.

Research Scholars Graduated in 2012-2013

PHD SCHOLARS

Name: Shyamosree Pal
Thesis Title: Curvature, Circularity, and Related Applications: A Digital Geometric Perspective
Supervisor: Prof. Partha Bhowmick

Name: Debi Prosad Dogra
Thesis Title: Algorithms for Video Assisted Analysis of Infant Neurological Examinations
Supervisor: Prof. Arun Kumar Majumdar, Prof. Shamik Sural

Name: Arnab Sarkar
Thesis Title: New Approaches in Real-Time Proportional Fair Multi-Processor Scheduling
Supervisor: Prof. Sujoy Ghose

Name: Chandan Karfa
Thesis Title: Formal Verification of Behavioural Transformations During Embedded System Design
Supervisor: Prof. Chittaranjan Mandal, Prof. Dipankar Sarkar

Name: Joydeep Chandra
Thesis Title: Topology and its Effects on the Performance of Peer-to-Peer Networks
Supervisor: Prof. Niloy Ganguly

Name: Subhankar Mukherjee
Thesis Title: Assertions: From a Mixed-Signal Perspective
Supervisor: Prof. Pallab Dasgupta, Prof. Siddhartha Mukhopadyhay

Name: Pravanjan Choudhury
Thesis Title: New Multiprocessor Scheduling Techniques for Dynamic Task Graphs
Supervisor: Prof. P.P. Chakrabarti, Prof. Rajeev Kumar

Name: Soumen Bag
Thesis Title: Processing and analysis of Bangla optical characters using geometric and topological features
Supervisor: Prof. Gaurav Harit, Prof. Partha Bhowmick

Name: Dinesh Dash
Thesis Title: Geometric algorithms for coverage in wireless sensor networks
Supervisor: Prof. Anupam Basu, Prof. Arobinda Gupta

MS SCHOLARS

Name: Sourasis Das
Thesis Title: Formal Methods for Improving Test and Assertion Coverage
Supervisor: Prof. Pallab Dasgupta, Prof. Partha Pratim Das

Name: Pramit Roy
Thesis Title: Misbehavior Detection in Vanet Using Secondary Information
Supervisor: Prof. Arobinda Gupta

Name: Sujoy Sinha Roy
Thesis Title: Design and Analysis of Elliptic Curve Cryptography Algorithms on FPGAs
Supervisor: Prof. Debdeep Mukhopadhyay

Name: Suprabhat Das
Thesis Title: Search and quantitative analysis of Rabindra Rachanabali collection
Supervisor: Prof. Pabitra Mitra

Name: Sumit Das
Thesis Title: Computational Approach Improving Fluency in Bangla Sentence Generation
Supervisor: Prof. Anupam Basu

Name: Sourya Bhattacharyya
Thesis Title: Computational Approach Improving Fluency in Bangla Sentence Generation
Supervisor: Prof. Arun Kumar Majumdar, Prof. Jayanta Mukhopadhyay

Name: Animesh Srivastava
Thesis Title: Impact of Attacks on Correlated P2P Network Topology: A Complex Network Approach
Supervisor: Prof. Niloy Ganguly

Name: Biswajit Das
Thesis Title: Automatic Speech Recognition of Aging Speech in Bengali
Supervisor: Prof. Pabitra Mitra

Name: Debjit Pal
Thesis Title: Automated Mixed-Signal Verification Using Monitors and Simulation Relations
Supervisor: Prof. Pallab Dasgupta, Prof. Siddhartha Mukhopadyhay

Name: Satrajit Ghosh
Thesis Title: Improvements of Linearization-Based Algebraic Attacks on Block Ciphers
Supervisor: Prof. Abhijit Das

Name: Chandan Misra
Thesis Title: A software system for transcribing and rendering indic music system
Supervisor: Prof. Anupam Basu, Prof. B. Bhattacharya (CE)

Awards and Achievements

- *Bodhisatwa Mazumdar* received the Best Student Paper award in 25th International Conference on VLSI Design 2012.
- *Joydeep Chandra* received the Best Paper Award at IEEE TrustCom 2012.
- *Parantapa Bhattacharya* and *Saptarshi Ghosh*'s joint poster gets first prize at Microsoft TechVista 2013.
- *Rajdeep Mukherjee* received the Best Paper Award at PrimeAsia 2012.
- *Rishiraj Saha Roy* won the Best Poster Award at the 9th International Conference on the Evolution of Language (Evolang 9), 2012.

- *Maunendra Sankar Desarkar* gets best PhD presentation award in 2nd IDRBT Doctoral Colloquium 2012.
- *Saptarshi Ghosh* and *Maunendra Sankar Desarkar* received Honorable Mention Awards in Yahoo Key Scientific Challenges Program in 2012.
- *Tanmoy Chakraborty* and *Sandipan Sikdar*'s joint poster gets Honorable Mention at Microsoft TechVista 2013.
- *Subhadip Kundu*'s paper gets nomination for best paper award at 50th ACM/IEEE Design Automation Conference (DAC), 2013.

- *Kunal Banerjee*, *Soumyadip Bandyopadhyay* and *Tanwi Mallick* received TCS Research Scholarship in 2012.
- *Sandip Karmakar* received Microsoft Research India PhD Fellowship in 2012.
- *Tanmoy Chakraborty* received Google India PhD Fellowship in 2012.

Publications by Research Scholars (2012-2013)

2013

1. A. Hazra, P. Ghosh, S. G. Vadlamudi, P. P. Chakrabarti and P. Dasgupta; Formal Methods for Early Analysis of Functional Reliability in Component-Based Embedded Applications; Accepted for Publication in IEEE Embedded Systems Letters (ESL), 2013.
2. A. Hazra, S. Goyal, P. Dasgupta and A. Pal; Formal Verification of Architectural Power Intent; In the IEEE Transactions on Very Large Scale Integration Systems (TVLSI), vol. 21, no. 1, pp. 78-91, 2013.
3. A. K. Singh, S. Dhal, I. Sengupta, An Approach to Solve Tracking and Message Blocking Problems in RFID in Proceedings of the 4th International Conference on Communications Security and Information Assurance, 2013 (accepted),
4. J. C. Mukherjee, and A. Gupta, "A Publish-Subscribe Based Framework for Event Notification in Vehicular Environments", Fifth International Conference on Communication Systems and Networks (COMSNETS), Bangalore, India, 2013.
5. P. Mondal, P. Desai, S. K. Ghosh, and J. Mukhopadhyay, " An Efficient SMS-Based Framework for Public Health Surveillance", IEEE EMBS Special Topic Conference on Point-of-Care Healthcare Technologies, pp. 244-247, 2013.
6. P. Nagaraju, R. Naskar and R. S. Chakraborty, "Improved Histogram Bin Shifting based Reversible Watermarking", accepted in International Conference on Intelligent System and Signal Processing (ISSP) 2013, Gujarat, India.
7. R. Mukherjee, P. Dasgupta, A. Pal, S. Mukherjee - "Formal Verification of Hardware / Software Power Management Strategies", In International Conference on VLSI Design, (VLSID) 2013.
8. R. Mukherjee, S. Mukherjee, P. Dasgupta - " Model Checking Global Power Management Strategies in Software with safety LTL properties", In International Conference of Indian Software Engineering Conference, (ISEC) 2013.
9. R. Saha Roy, "Analyzing Linguistic Structure of Web Search Queries", in Ph.D. Symposium of the 22nd International World Wide Web Conference (WWW '13), Rio de Janeiro, Brazil, 13 - 17 May 2013.
10. R. S. Chakraborty, I. Saha, A. Palchaudhuri and G. K. Naik, "Hardware Trojan Insertion by Direct Modification of FPGA Configuration Bitstream", accepted for publication in IEEE Design and Test of Computers.
11. S. Ghosh, S. Agarwal, H. Srivastava, A. Mukherjee, "Run-time Delays in Indian Railways: is Traffic the Cause?", ACM Symposium on Computing for Development (DEV), Bangalore, India, January 2013.
12. S. Ghosh, S. Saha, A. Srivastava, T. Krueger, N. Ganguly, A. Mukherjee, "Understanding Evolution of Inter-Group Relationships using Bipartite Networks", IEEE Journal on Selected Areas in Communications (JSAC) – Special Issue on Emerging Technologies in Communications (accepted).
13. S. Khurana, S. Kolay, C. Rebeiro, and D. Mukhopadhyay, "Lightweight Cipher Implementations on Embedded Processors", accepted in DTIS 2013.
14. S. Kumar, S. Roy, P. P. Chakrabarti, B. B. Bhattacharya and K. Chakrabarty, "Efficient Mixture Preparation on Digital Microfluidic Biochips", accepted for publication in the Sixteenth IEEE Symposium on Design and Diagnostics of Electronic Circuits and Systems (DDECS), 2013.

15. S. Kundu, A. Jha, S. Chattopadhyay, I. Sengupta and R. Kapur, “A Framework for Multiple Fault Diagnosis based on Multiple Fault Simulation using Particle Swarm Optimization”, accepted in IEEE Transactions on Very Large Scale Integration Systems (TVLSI), February 2013.

16. S. Kundu, S. Chattopadhyay, I. Sengupta and R. Kapur, “Aggressive Scan Chain Masking for Improved Diagnosis of Multiple Scan Chain Failures”, accepted in IEEE European Test Symposium (ETS), 2013.

17. S. Kundu, S. Chattopadhyay, I. Sengupta and R. Kapur, “An ATE Assisted DFD Technique for Volume Diagnosis of Scan Chains”, accepted in 50th ACM/IEEE Design Automation Conference (DAC), 2013.

18. S. K. Maity, T.V. Manoj and A. Mukherjee, “Opinion formation in time-varying social networks: The case of Naming Game”, Physical Review E, 86, 036110.

19. S. Prabhu M, A. Hazra and P. Dasgupta; Reliability Guarantees in Automata Based Scheduling for Embedded Control Software; Accepted for Publication in IEEE Embedded Systems Letters (ESL), 2013.

20. S. Saha and N. Ganguly, “Coverage maximization under resource constraints using a non-uniform proliferating random walk”, accepted for publication in Physical Review E.

21. X. Wang, 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”, to appear in Design Automation Conference (DAC), 2013.

2012

1. A. Chakrobarty, S. Ghosh, N. Ganguly, “Detecting Overlapping Communities in Folksonomies”, ACM Hypertext Conference, Milwaukee, USA, June 2012.
2. A. De, M. S. Desarkar, N. Ganguly, and P. Mitra, “Local learning of item dissimilarity using content and link structure,” Proc. ACM Conf. Recommender Systems (RecSys 2012), Dublin, 221-224.
3. A.D. Choudhury, A.K. Agrawal, P. Sinha, C. Bhaumik, A. Ghose, S. Bilal, "A methodology for GPS-based waterlogging prediction and smart route generation", 12th International Conference on Intelligent Systems Design and Applications (ISDA), 2012
4. A. Dhar, S. Chatterji, S, Sarkar, A, Basu, “A Hybrid Dependency Parser for Bangla”, In Proceedings of the 10th Workshop on Asian Language Resources, pages 55–64, COLING 2012, Mumbai, December 2012.
5. A. Hazra, P. Dasgupta and P. P. Chakrabarti, “Cohesive Coverage Management Leveraging Formal Test Plans”, LAP LAMBERT Academic Publishers, January 2012 (ISBN: 978-3-8473-7645-3).
6. A. Hazra, P. Dasgupta, A. Banerjee and K. Harer, “Formal Methods for Coverage Analysis of Architectural Power States in Power-Managed Designs”, In the 17th Asia and South Pacific Design Automation Conference (ASP-DAC), pp. 585-590, January 2012.
7. A. Hazra, P. Ghosh and P. Dasgupta, “Reliability Annotations to Formal Specifications of Context-Sensitive Safety Properties in Embedded Systems”, In the Forum on Specification and Design Languages (FDL), pp. 36-43, September 2012.
8. A. Hazra, P. Ghosh, P. Dasgupta and P. P. Chakrabarti, “Cohesive Coverage Management: Simulation meets Formal”, In the Journal of Electronic Testing: Theory and Applications (JETTA), vol. 28, no. 4, pp. 449-468, 2012.
9. B. Ghoshal, S. Kundu, I. Sengupta, S. Chattopadhyay, “Particle Swarm Optimization Based BIST Design for Memory Cores in Mesh Based Network-on-Chip”, VDAT 2012: 343-349.
10. C. Bhaumik, A.K. Agrawal, P. Sinha, "Using social network graphs for search space reduction in internet of things", Proceedings of the 2012 ACM Conference on Ubiquitous Computing (Ubicomp), 2012.
11. C. Rebeiro and D. Mukhopadhyay, "A Formal Analysis of Prefetching in Profiled Cache Timing Attacks", Poster in the 14th International Workshop on Cryptographic Hardware and Embedded Systems, CHES 2012, Leuven, Belgium.
12. C. Rebeiro and D. Mukhopadhyay, "Boosting Profiled Cache Timing Attacks with Apriori Analysis", accepted in IEEE Transactions Information Forensics and Security, Volume 7, Issue 6, pp 1900-1905, 2012.
13. C. Rebeiro, S. S. Roy, and D. Mukhopadhyay, "Pushing the Limits of High-Speed GF(2^m) Elliptic Curve Scalar Multiplication on FPGAs", in the Proceedings of the 14th International Workshop on Cryptographic Hardware and Embedded Systems, CHES 2012, Leuven, Belgium, pp 494-511, LNCS 7428.
14. D. Basu Roy and D. Mukhopadhyay, “An Efficient High Speed Implementation of Flexible Characteristic-2 Multipliers on FPGAs”, appeared in VDAT 2012.

15. D. Mitra, S. Roy, K. Chakrabarty and B. B. Bhattacharya, "On-Chip Sample Preparation with Multiple Dilutions Using Digital Microfluidics", in Proceedings of the IEEE International Symposium on VLSI (ISVLSI), pp. 314-319, August 19-21, 2012, Amherst, USA.

16. K. Banerjee, C. Karfa, D. Sarkar, and C. Mandal, "A Value Propagation Based Equivalence Checking Method for Verification of Code Motion Techniques", International Symposium on Electronic System Design (ISED), December 2012, pp: 67-71.

17. K. Ghosh, P. Dasgupta, S. Ramesh, "Planning with action prioritization and new benchmarks for classical planning," in Proceedings of the 25th Australasian Joint Conference on Artificial Intelligence, pp 779–790, 2012.

18. M. S. Desarkar and S. Sarkar, "Preference Relation Based Matrix Factorization for Recommender Systems", in 20th International Conference on User Modeling, Adaptation, and Personalization (UMAP), Montreal, 2012.

19. M. S. Desarkar and S. Sarkar, "Rating prediction using preference relations based matrix factorization". FactMod Workshop in 20th International Conference on User Modeling, Adaptation, and Personalization (UMAP), Montreal, 2012.

20. M. S. Desarkar and S. Sarkar, "User based Collaborative Filtering with Temporal Information for Purchase Data", International Conference on Knowledge Discovery and Information Retrieval (KDIR), Barcelona, 2012.

21. M. Sinha, A. Jana, T. Dasgupta, A. Basu, "A New Semantic Lexicon and Similarity Measure in Bangla", International Conference on Computational Linguistics (COLING), Workshop on Cognitive Aspects of the Lexicon (CogALex-III), 2012, pp-171-182.

22. M. Sinha, S. Sharma, T. Dasgupta, A. Basu, "A New Readability Measure of Bangla and Hindi Texts", International Conference on Computational Linguistics (COLING), 2012, pp-1141-1150.

23. M. Sinha, T. Dasgupta and A. Basu, "A Complex Network Analysis of Syllables in Bangla through SyllableNet", International Conference on Language Resources and Evaluation (LREC), Workshop on Indian Language and Data: Resources and Evaluation (WILDRE), 2012.

24. N. Ganguly, S. Ghosh, T. Krueger, A. Srivastava, "Degree Distributions of Evolving Alphabetic Bipartite Networks and their Projections", Theoretical Computer Science, Elsevier, vol. 466, pp. 20-36, December 2012.

25. N. Phuong Ha, C. Rebeiro, D. Mukhopadhay, and W. Huaxiong, "Improved Differential Cache Trace Attacks on SMS4", Inscrypt 2012.

26. N. Sharma, S. Ghosh, F. Benevenuto, N. Ganguly, K. Gummadi, "Inferring Who-is-Who in the Twitter Social Network", Workshop on Online Social Networks (WOSN), Helsinki, Finland, August 2012.

27. P. Ghosh, A. Hazra, R. Gonnabhaktula, N. Bhilegaonkar, P. Dasgupta, C. Mandal and K. Paul; POWER-SIM : An SOC Simulator for Estimating Power Profiles of Mobile Workloads; In the Journal of Low-Power Electronics (JOLPE), vol. 8, no. 3, pp. 293-303, 2012.

28. P. Mondal, J. Mukhopadhyay, S. Sural, A. K. Majumdar, B. Majumdar, S. Mukherjee, and A. Singh , "A Robust Method for Ventriculomegaly Detection from Neonatal Brain Ultrasound Images", International Journal of Medical Systems, vol. 36, no. 5, pp 2817-2828, 2012.

29. P. Mondal, J. Mukhopadhyay, S. Sural, and P. P. Bhattacharyya, "An Efficient Model-Guided Framework for Alignment of Brain MR Image Sequences", IEEE International Conference on Systems, Man, and Cybernetics, pp. 2201-2206, 2012.

30. P. Mondal, J. Mukhopadhyay, S. Sural, and P. P. Bhattacharyya, “High Resolution 3-D MR Image Reconstruction from Multiple Views”, The Eighth Indian Conference on Vision, Graphics and Image Processing, pp. 1-8 (4), 2012.

31. P. Sinha, A. Ghose and C.Bhaumik, "City Soundscape". Poster. ACM Proceedings of 13th Annual International Conference on Digital Goverment Research, Maryland, June 2012.

32. R. Mukherjee, P. Ghosh, A. Pal, “Hotspot Reduction using Fine-grained DVS Architecture at 90 nm Technology”, In Asia-Pacific Conference on Postgraduate Research in Microelectronics & Electronics, (PRIMEASIA) 2012.

33. R. Mukherjee, P. Ghosh, N. S. Kumar, P. Dasgupta, A. Pal - “Multi-Objective Low-power CDFG Scheduling using Fine-Grained DVS Architecture in Distributed Framework”, In International Symposium of Electronic Design, (ISED) 2012.

34. R. Mukherjee, P. Ghosh, P. Dasgupta, A. Pal, “A Multi-Objective Perspective for Operator Scheduling using Fine-Grained DVS Architectures”, In International Journal of VLSI design & Communication Systems (VLSICS Journal), 2012.

35. R. Mukherjee, P. Ghosh, P. Dasgupta, A. Pal, “Operator Scheduling Revisited: A Multi-Objective Perspective for Fine-Grained DVS Architecture”, in proceedings of the International Conference on Advances in Computing and Information Technology, (AC-ITY) 2012.

36. R. Naskar and R. S. Chakraborty, "A Generalized Tamper Localization Approach for Reversible Watermarking Algorithms", accepted for publication in ACM Transactions on Multimedia Computing Communications and Applications.

37. R. Naskar and R. S. Chakraborty, "Fuzzy Inference Rule based Reversible Watermarking for Digital Images", International Conference on Information Systems Security (ICISS), Guwahati, India, 2012. Published in Lecture Notes on Computer Science, vol. 7671, pp. 149-163, 2012.

38. R. Naskar and R. S. Chakraborty, "Histogram–Bin–Shifting based Reversible Watermarking for Color Images", accepted for publication in IET Image Processing.

39. R. Naskar and R. S. Chakraborty, "Lossless Secret Image Sharing based on Generalized–LSB Replacement", ACM Research in Applied Computation Symposium (RACS), San Antonio, Texas, USA, 2012.

40. R. Saha Roy, M. Choudhury and K. Bali, "Are Web Search Queries an Evolving Protolanguage?", in Proceedings of the 9th International Conference on the Evolution of Language (Evolang IX), 13 - 16 March 2012, Kyoto, Japan, pages 304 – 311 [BEST RESEARCH POSTER AWARD].

41. R. Saha Roy, N. Ganguly, M. Choudhury and S. Laxman, "An IR-based Evaluation Framework for Web Search Query Segmentation", in Proceedings of the 35th Annual ACM SIGIR Conference on Research and Development on Information Retrieval (SIGIR '12), Portland, USA, 12 - 16 August 2012, pages 881 – 890.

42. S. Bandyopadhyay, K. Banerjee, D. Sarkar and C. Mandal, “Translation Validation for PRES+ Models of Parallel Behaviours via an FSMD Equivalence Checker”, International Symposium on VLSI Design and Test (VDAT), July 2012, pp: 69 -78.

43. S. Bhattacharya, C. Rebeiro, and D. Mukhopadhyay, "Hardware Prefetchers Leak : A Revisit of SVF for Cache-Timing Attacks", accepted in HASP 2012 (held in conjunction with MICRO-45).

44. S. Burman, A. Palchaudhuri, R. S. Chakraborty, D. Mukhopadhyay and P. Singh, “Effect of Malicious Hardware Logic on Circuit Reliability”, International Symposium on VLSI Design

and Test (VDAT) 2012, Shibpur, India. Published in Lecture Notes on Computer Science, vol. 7373, pp. 190-197, 2012.

45. S. Chatterji, A. Dhar, S. Sarkar, A. Basu, "A Three Stage Hybrid Parser for Hindi", In Proceedings of the Workshop on Machine Translation and Parsing in Indian Languages (MTPIL-2012), pages 155–162, COLING 2012, Mumbai, December 2012.

46. S. Chatterji, A. Dhar; S. Sarkar, A. Basu, "Translations of Ambiguous Hindi Pronouns to Possible Bengali Pronouns", in Proceedings of the 10th Workshop on Asian Language Resources, pages 125–134, COLING 2012, Mumbai, December 2012.

47. S. Chatterji, D, Chatterjee, S, Sarkar, "An Efficient Technique for De-Noising Sentences using Monolingual Corpus and Synonym Dictionary", in Proceedings of COLING 2012: Demonstration Papers, Mumbai, India, December, 2012, pp 59-66.

48. S. Chatterji, N. Datta, A. Dhar, B. Barik, S. Sarkar, A. Basu, "Repairing Bengali Verb Chunks for Improved Bengali to Hindi Machine Translation", in Proceedings of the 10th Workshop on Asian Language Resources, pages 65–74, COLING 2012, Mumbai, December 2012.

49. S. Dhal, I. Sengupta, "A New Authentication Protocol for Multi-tag RFID Applicable to Passiven Tag" in Proceedings of the 2nd International Conference on Communication, Computing & Security, 2012, pp. 880-888.

50. S. Dhal, I. Sengupta, "A New Authentication Protocol for Multi-tag RFID" in Proceedings of the 1st International Conference on Recent Advances in Information Technology, 2012.

51. S. Ghosh, A. Banerjee, N. Ganguly, "Some Insights on the Recent Spate of Accidents in Indian Railways", Physica A: Statistical Mechanics and its Applications, Elsevier, vol. 391, issue 9, pp. 2917-2929, 2012.

52. S. Ghosh, A. Srivastava, N. Ganguly, "Effects of a Soft Cut-off on Node-degree in the Twitter Social Network", Computer Communications, Elsevier, vol. 35, issue 7, pp. 784-795, 2012.

53. S. Ghosh, B. Viswanath, F. Kooti, N. Sharma, G. Korlam, F. Benevenuto, N. Ganguly, K. Gummadi, "Understanding and Combating Link Farming in the Twitter Social Network", ACM World Wide Web Conference (WWW), Lyon, France, April 2012.

54. S. Ghosh, N. Sharma, F. Benevenuto, N. Ganguly, K. Gummadi, "Cognos: Crowdsourcing Search for Topic Experts in Microblogs", ACM SIGIR Conference, Portland, USA, August 2012.

55. S. Ghoshal, D. Mitra, S. Roy, and D. D. Majumder, "Chapter 9: Advance in Biosensors and Biochips", Modern Sensors, Transducers and Sensor Networks (Book Series: Advances in Sensors: Reviews, Vol. 1), Sergey Y. Yurish(ed.), ISBN:978-84-615-9012-4, pp. 9:1-9:33, International Frequency Sensor Association (IFSA) Publishing, May, 2012.

56. S. G. Vadlamudi, P. Gaurav, S. Aine, P. P. Chakrabarti, "Anytime Column Search", 25th Australasian Joint Conference on Artificial Intelligence (AI), LNCS, vol.7691 (AI 2012: Advances in Artificial Intelligence), pp.254-265, 4-7 Dec. 2012, Sydney, Australia.

57. S. G. Vadlamudi, P. P. Chakrabarti, S. Sarkar, "Anytime Algorithms for Mining Groups with Maximum Coverage", 10th Australasian Data Mining Conference (AusDM), CRPIT, vol.134 (Data Mining and Analytics 2012), pp.209-219, 5-7 Dec. 2012, Sydney, Australia.

58. S. Karati, A. Das, D. Roychowdhury, B. Bellur, D. Bhattacharya and A. Iyer, "Batch verification of ECDSA signatures", 5th International Conference on Cryptology in Africa (AfricaCrypt 2012), Lecture Notes in Computer Science #7374, pp 1-18, Jul 10-12, 2012, Ifrane, Morocco.

59. S. Karmakar, D. Roy Chowdhury: “Countermeasures of Side Channel Attacks on Symmetric Key Ciphers using Cellular Automata”, ACRI 2012.

60. S. Karmakar, D. Mukhopadhayay, D. Roy Choudhury: CAvium, “Strengthening Trivium using Cellular Automata”, Journal of Cellular Automata.

61. S. K. Dandapat, B. Mitra, R. Roychoudhury, and N. Ganguly, "Framework for Collaborative Download in Wireless Mobile Environment", IEEE Mobile Data Management , Bangalore, India, July, 2012 (PhD Forum).

62. S. K. Dandapat, B. Mitra, R. Roychoudhury, and N. Ganguly, "Smart Association Control In Wireless Mobile Environment Using Max-Flow", IEEE Transaction on Network and Service Management 2012.

63. S. K. Dandapat, S. Jain, R. Roychoudhury, and N. Ganguly, "Distributed Content Storage for Just-in-Time Streaming," ACM, SIGCOMM , Helsinki, Phinland, August 2012 (Poster).

64. S. K. Maity, and A. Mukherjee, “Understanding how dominance affects the emergence of agreement in a social network: The case of Naming Game,” In the proceedings of 2012 IEEE/ASE International Conference on Social Computing, Amsterdam, The Netherlands.

65. S. Krishna Kumar, S. Kundu, S. Chattopadhyay, “Customizing completely specified pattern set targeting dynamic and leakage power reduction during testing”, Integration :45(2): 211-221 (2012).

66. S. Kundu, S. Chattopadhyay, I. Sengupta and R. Kapur, “A Diagnosability Metric for Test Set Selection targeting better Fault Detection”, in 25th IEEE International Conference on VLSI Design (VLSID), 2012.

67. S. Kundu, S. Chattopadhyay, “Efficient don't care filling and scan chain masking for low-power testing”, IJCAET 4(2): 101-125 (2012).

68. S. Kundu, S. Chattopadhyay; Strategies to Reduce Power during VLSI Circuit Testing; LAP LAMBERT Academic Publishers, September 2012 (ISBN: 978-3-659-25530-5).

69. S. Mishra, J. Mukherjee, P. Mondal, S. M. Aswatha, and J. Mukhopadhyay, “Real-time Retrieval System for Heritage Images”, International Conference on Emerging Research in Electronics, Computer Science and Technology, Accepted, 2012.

70. S. Mukhapadyay, T. Dasgupta and A. Basu, “Development of an Online Repository of Bangla Literary Texts and its Ontological Representation for Advance Search Options”, International Conference on Language Resources and Evaluation (LREC), Workshop on Indian Language and Data: Resources and Evaluation (WILDRE), 2012.

71. 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.

72. S. Pratihar, P. Bhowmick, S. Sural and J. Mukhopadhyay , “Detection and Removal of Hand-drawn Underlines in a Document Image Using Approximate Digital Straightness”, Workshop on Document Analysis and Recognition (DAR), IIT Bombay, pages 124-131, ACM, 2012.

73. S. Pyne and A. Pal, “Branch Target Buffer Energy Reduction Through Efficient Multiway Branch Translation Techniques”, Journal of Low Power Electronics, Vol. 8, No. 5, 2012.

74. S. Roy, B. B. Bhattacharya, S. Ghoshal, and K. Chakrabarty, "Low-Cost Dilution Engine for Sample Preparation using Digital Microfluidic Biochips", in Proceedings of the Third International Symposium on Electronic System Design (ISED), pp. 203-207, December 19-22, 2012, Kolkata, India.

75. S. Roy, D. Mitra, B. B. Bhattacharya, and K. Chakrabarty, "Congestion-aware layout design for high-throughput digital microfluidic biochips", ACM Journal on Emerging Technologies in Computing Systems (JETC), Vol. 8, Issue 3, Article 17, August, 2012. Digital Object Identifier: 10.1145/2287696.2287700.

76. S. Roy, P. P. Chakrabarti and B. B. Bhattacharya, "Algorithms for On-Chip Solution Preparation using Digital Microfluidic Biochips", in Proceedings of the IEEE International Symposium on VLSI (ISVLSI), pp. 7-8, August 19-21, 2012, Amherst, USA. Digital Object Identifier: 10.1109/ISVLSI.2012.79.

77. S. Saha, R. Kumar and G. Baboo, “Characterization of graph properties for improved Pareto fronts using heuristics and EA for bi-objective graph coloring problem”, Applied Soft Computing, ASOC-1644, Accepted (2012).

78. S. Saha, N. Ganguly and A. Mukherjee, “Information Dissemination Dynamics in Delay Tolerant Network: A Bipartite Network Approach”, Third International Workshop on Mobile Opportunistic Networks ACM MobiOpp, Zurich, Switzerland, March 15-16, 2012.

79. S. Saha, N. Ganguly and A. Mukherjee, “Understanding Information Dissemination Dynamics in Delay Tolerant Networks using Theory of Bipartite Networks”, PhD Forum, COMSNETS, Bangalore, India, Jan 3-7, 2012.

80. S. Srinivasan, T. Chakraborty, and S. Bhowmick, “Identifying base clusters and their application to maximizing modularity”. Contemporary Mathematics. Graph partitioning and Graph Clustering. (D. A. Bader, H. Meyerhenke, P. Sanders and D. Wagner eds.), AMS-DIMACS, 2012.

81. S. S. Roy, C. Rebeiro, and D. Mukhopadhyay, "A Parallel Architecture for Koblitz Curve Scalar Multiplications on FPGA Platforms", accepted in IEEE 15-th Euromicro Conference on Digital System Design, Turkey, 2012.

82. S.S. Roy, C. Rebeiro, and D. Mukhopadhyay, "Theoretical Modeling of Elliptic Curve Scalar Multiplier on LUT Based FPGAs for Area and Speed", accepted in IEEE Transactions on Very Large Scale Integration Systems, April 2012.

83. S.S. Roy, C. Rebeiro, and D. Mukhopadhyay, "Generalized High Speed Itoh-Tsujii Multiplicative Inversion Architecture for FPGAs", accepted in Integration, the VLSI Journal, Elsevier, January 2012.

84. T. Dasgupta, A. Anuj, M. Sinha, R. Ghose, A. Basu, “VoiceMail Architecture in Desktop and Mobile Devices for the Blind People” IEEE International Conference on Intelligent Human Computer Interaction (IHCI), 2012.

85. T. Dasgupta, M. Sinha, A. Basu, "Computational Models to understand the Access and Representation of Bangla Polymorphemic Words in the Mental Lexicon", International Conference on Computational Linguistics (COLING), 2012, pp-235-244.

86. T. Dasgupta, M. Sinha, A. Basu, "Forward Transliteration of Dzongkha Text to Braille", International Conference on Computational Linguistics (COLING), Workshop on Advances in Text Input Mechanisms, 2012, pp-97-106.

87. T. Dasgupta, S. Mukherjee, M. Sinha, and A. Basu, “Compound Verb Identification in Bangla”, International Conference on Computational Linguistics (COLING), Workshop on South and Southeast Asian Natural Language Processing (SANLP), 2012, pp-153-162.

88. T. K. Maiti, S. Kundu, A. Dutta and S. Chattopadhyay, “Confidence based power aware testing”, in ISED 2012.

89. T. Sen and R. Mall, A model based approach to regression test selection of Component based software. In Proceedings of the 2012 Workshop on Advances in Model Based Software Engineering, held in IIT Kanpur, India, February 2012.

90. T. Sen and R. Mall, State Model Based Regression Test Reduction for Component based Software. In ISRN Journal of Software Engineering, 2012.

91. V. Shrivastav, S. G. Vadlamudi, P. P. Chakrabarti, D. Das, P. Sinha, “Finding Critical Components in Embedded Control Systems Sensitive to Quality-Faults”, 3rd International Symposium on Electronic System Design (ISED), IEEE, pp.167-171, 19-22 Dec. 2012, Kolkata, India.

Indian Institute of Technology Kharagpur