

Teaching Statement

SOURADYUTI PAUL

December 5, 2007

Katholieke Universiteit Leuven,
Electrical Engineering Department,
Kasteelpark Arenberg 10, B-3001, Belgium.

Tel: +32-16-328663 Fax: +32-16-321969
Email: Souradyuti.Paul@esat.kuleuven.be
<http://homes.esat.kuleuven.be/~psourady>

1 Introduction

It is sometimes mistakenly assumed that the main beneficiary of good teaching are the students. In reality, the teachers themselves benefit more than the students in their strives to excel at teaching in classrooms. While a student can afford to neglect some parts of curricula not considered important from the exams' point of view and get away with good grades without them, an honest teacher can hardly allow such omissions in her teaching preparations lest she may face grave embarrassments at the hands of a nitpicky student. I grew up in a teaching climate where I got used to the sight of a man, my father, a former professor of mathematics in a college, burning the midnight oil in his painstaking preparation to make lecture notes for the students. Little did I know at that time that such a passion for teaching that I observed from very close quarters would, later on, help me to make a choice about my future profession.

There is no doubt in my mind that teaching is an integral part of research. Teaching allows an academician to tie the loose ends of her research, to enlarge her vision of a subject which, at times, gets narrowed unknowingly by a single minded focus on a highly specialized research topic and, also, to acquire knowledge directly by interacting with the fresh and active minds of the students. In addition to the above gains which are somewhat materialistic, there is another source of satisfaction in a teaching profession that is, to some extent, spiritual and, perhaps, has made this profession one of the most noble and respected ones. The satisfaction is derived from the successful discharge of a responsible social duty of educating the future generations. For some, the satisfaction of a research-cum-teaching profession can be so much that they can turn down plum job opportunities elsewhere to follow their dreams in academia. The author of this article is one of them who, in the past, left behind prospective offers from some of the global leaders in the software industry (Tata Consultancy Services, Novell, Sun Microsystems etc.) to make a career in the greener pastures of academic institutes.

2 Teaching Philosophy

Riding my deep rooted familial background in research-cum-teaching related professions¹ and my education in some well known institutes in India and abroad, I am fortunate to have been able to attend lectures delivered by a number of notable academicians across the globe – Prof. Bart Preneel, Prof. K. S. Vijayan, Prof. Adi Shamir, Prof. Amartya Kumar Sen, Prof. Manindra Agarwal, to name a few – who had helped me to develop an unambiguous and comprehensive idea about the qualities of a good teacher. Below I outline the criteria which I believe a teacher should possess in order to expect to leave a distinct mark in teaching profession.

- **The motivation factor.** I believe that one of the most important qualities of a teacher is her ability to motivate the students into their learning process. It is often said that nothing can be taught unless the student is willing to learn. It is definitely incumbent on the teachers to create a perfect atmosphere for the students to learn with ease, joy and enthusiasm. It is sometimes the case that, due to lifeless presentation of a subject, the pupils are scared away from it right from the beginning. To draw the students into a subject, a teacher should take adequate care such that the subject is presented in an interesting way. (1) Presentation of a topic with simple examples, (2) clarity of explanation and (3) expounding a subject with its practical usefulness are some of the ways, which I think, a teacher should follow to interest the students in a subject; a detailed description of them, however, requires a separate discussion.
- **Encouragement for brainstorming.** Rather than spoon feeding bookish solutions to the students all the time, to instil ideas in their minds in perspective, in my opinion, a useful technique is to, first, allow them to brainstorm problems independently. Such brainstorming process binds the students strongly to the subject, at the same time it leaves open the possibility of emergence of new and original ideas from them. It is, however, noteworthy that some of the excellent achievements in several scientific disciplines are known to have had been initiated in Master's theses.
- **Fostering creative excellence rather than competitive excellence.** In my career so far, as a student as well as a researcher at several institutes, it was a great pain for me to observe many creative talents having been ruined under the demands of the academic system for competitive excellence rather than creative excellence. As a teacher, therefore, I never refrain from employing efforts to protect and promote the creative impulses of the students. A very effective way to achieve that is to attach more credits to project related works than to exams.
- **Interaction.** Last but never the least, it is important for a teacher to interact with the students in and out of the classroom over issues, not necessarily always academic, to strike a friendly relation with them. A coach brings out the best in a student as a friend not as a boss. This, however, should not amount to sparing the rod and spoiling the child.

¹My father, grandmother, uncle etc. are in teaching related jobs.

3 Teaching Expertise

Although my main research topic is cryptology, i.e., the science of hiding information from the unauthorized users and making them re-available to the authorized ones with the help of ciphers, I'm also interested in study and analysis of algorithms in other branches of computer science such as complexity theory, models of computation, algorithmic graph theory and coding theory. The above subjects had been my favorites during my student days. At present the following courses are the ones I am able to teach.

- *Master's Level:* Introduction to Algorithms, Data Structures, Automata Theory, Computer Architectures, Software Engineering, Combinatorics, Discrete Mathematics, Introduction to Cryptology.
- *Doctoral Level:* Design and Analysis of Symmetric Ciphers (stream ciphers, block ciphers, hash functions and MACs).

4 Supervising and Teaching Experiences

The teaching and the supervising experiences I gathered are discussed below.

Supervising. I supervised the following Master's theses.

- Gorka Munduate, ERASMUS STUDENT in KULeuven, University of UPV/EHU, Basque Country, Spain, "Cryptanalysis of the Stream Cipher RC4A," 2004–2005.
- Gautham Sekar, Visitor to ESAT in KULeuven, Master's Student, Birla Institute of Technology, Pilani, India, "Cryptanalysis of the Stream Cipher Py," July–Dec 2005.

When the supervising experience has proved to be immensely beneficial to my own research, I also believe that Gorka and Gautham had pleasant academic experiences working with me too. It is also important to note that Gautham's thesis resulted in a publication in Lecture note in Computer Science (presented at FSE 2006) and he was the recipient of *Dr. Ranjit Singh Chauhan Undergraduate Research Award for the year 2006–2007* for the thesis which I supervised.² As it turned out that Gautham, subsequently, opted to do a PhD in cryptology (research group: COSIC, K.U.Leuven) casting aside offers from other renowned universities. I believe that the factor of his working under my supervision had played a part in this career choice.

Teaching. To train the above master's level students from scratch up to the basic principles of cryptology, I gave the following two courses in order to prepare them for the theses.

²The award, instituted by an alumnus of BITS-Pilani, is aimed at enhancing the long term research potential of India in both basic and applied research. It is typically given to one student from among the entire undergraduate batch of BITS (spanning across all streams of science and engineering) and students who have completed their undergraduate studies from the university recently.

- Course titled “Overview of Symmetric Cryptology.”
 - July – August 2004 (four hours a week, five weeks).
 - July – August 2005 (four hours a week, five weeks).
- Course titled “Overview of Stream Cipher Cryptanalysis.”
 - August – September 2004 (two hours a week, four weeks).
 - August – September 2005 (two hours a week, four weeks).

I offered a short tutorial to the master’s level students of Korea University.

- A tutorial titled “Stream Ciphers in Cryptography” at the Center for Information Security Technologies (CIST), Korea University, August 2007.

My courses organized by K.U.Leuven COSIC within the framework of BCRYPT (a research consortium comprising a number of European Universities) are below.

- “Stream Ciphers in Cryptology-I,” Organized by K.U.Leuven COSIC within BCRYPT framework, Dec 2007.
- “Stream Ciphers in Cryptology-II,” Organized by K.U.Leuven COSIC within BCRYPT framework, March 2008.

5 Future Plans and Conclusions

In order to survive in this fast advancing technological world, an essential quality of an educator is to have the attitude to constantly update oneself, be it research or teaching. In teaching, I have plans to give courses on the recent advancements in side channel cryptanalysis, fault attacks and quantum cryptography, the areas which seem to take lead roles in cryptologic world in future.