Curriculum Vitae of Subhamoy Maitra

Contents

1 Academic and Professional Qualification

1.1 At Indian Statistical Institute

Name:	Subhamoy Maitra
Designation:	Professor (Higher Academic Grade) [July 2014 –]
	Professor [June 2008 – June 2014]
	Professor in Charge, Applied Statistics Division [September 2010 – August 2012]
	Associate Professor [July 2003 – May 2008]
	Computer Engineer* [April 1997 – June 2003]
	(* Lecturer equivalent permanent faculty position)
Address:	Applied Statistics Unit, Indian Statistical Institute, 203 B T Road, Kolkata 700 108, India.
(including e-mail & Ph. No.)	subho@isical.ac.in, +91-98303-77324

1.2 Details of Educational Qualification

- Secondary Examination (Std. X) in the year 1986 from West Bengal Board of Secondary Education with marks 80.6% and rank 63rd.
- Higher Secondary Examination (Std. XII) in the year 1988 from West Bengal Council of Higher Secondary Education with marks 87.7% and **rank 5th**.
- Bachelor of Engineering in Electronics & TeleCommunication from Jadavpur University, Calcutta (1988-1992) with marks 85.6% and rank 7th.
- Master of Technology in Computer Science from Indian Statistical Institute, Calcutta (1994-1996) with marks 90.7% and **rank 1st**. **Awarded the "Indian Statistical Institute Alumni Association Medal" for outstanding performance in M. Tech. (CS).**
- PhD from Indian Statistical Institute, thesis entitled "Boolean Functions with Important Cryptographic Properties", 2001.

2 List of publications (peer reviewed)

See the DBLP link at my webpage.

3 Externally Funded Projects

Served in Governmental and Industry sponsored projects worth INR 20 crores (approx. 4 million US$) in last 10 years.

4 Membership of reputed agency

Cryptology Research Society of India (CRSI)

5 Awards and recognitions

1. **Invited Speaker** in **Sequences & Their Applications (SETA) in China**, at Southwest Jiaotong University, Chengdu, China, 9-14 October, 2016.
2. DAE Science Research Council **Outstanding Investigator** award, 2014.
3. **Invited Tutorial Speaker** in **Indocrypt 2012** December 9-12, 2012, Kolkata, India.
4. **Invited Speaker** in the **first International Workshop on ZUC algorithm**, December 2-3, 2010, Beijing, China.
5. **Nominated from Japanese Ministry of Foreign Affairs (MOFA)** as one of the Indian experts to discuss co-operation possibilities between India and Japan in the areas of Biotechnology, Nanotechnology and Information and Communication Technology during October 16–17, 2006 at Tokyo, Japan.
6. **Invited Tutorial Speaker** in **ICISS 2006** December, 2006, Kolkata.
7. **Invited Speaker** in the **First National Cryptology Symposium in Turkey**, at Middle East Technical University (METU), Ankara, Turkey, during November 18-20, 2005.
8. **Program Co-Chair** of Indocrypt 2003 and Indocrypt 2005.
9. **General Chair** of FSE 2004.
10. **Editorial Board Member** of the International Journal **"Cryptography and Communications: Discrete Structures, Boolean Functions and Sequences"**, published by Springer.

6 Other Academic & Professional Information

6.1 Thesis Supervision

1. Dr. Deepak Kumar Dalai received his PhD degree (Title: On Some Necessary Conditions of Boolean Functions to Resist Algebraic Attacks) in Computer Science from Indian Statistical Institute in 2006.

2. Dr. Tanmoy Kanti Das received his PhD degree (Title: Analysis and Design of Digital Watermarking Schemes) in Computer Science in the year 2006 from Jadavpur University (co-supervisor: Prof. Debesh Das).

3. Dr. Sumanta Sarkar received his PhD degree (Title: Combinatorial Aspects in Construction of Cryptographically Significant Boolean Functions under different Symmetry Conditions) in Mathematics in the year 2008 from Jadavpur University.

4. Dr. Goutam Paul received his PhD degree (Title: Analysis and Design of RC4 and its Variants) in Computer Science in the year 2009 from Jadavpur University.

5. Dr. Santanu Sarkar received his PhD degree (Title: Some Results on Cryptanalysis of RSA and Factorization) in Mathematics in the year 2011 from Indian Statistical Institute.

6. Dr. Pinaki Sarkar received his PhD degree (Title: Applications of Mathematics and Cryptology in Wireless Sensor Networks) in Mathematics in the year 2013 from Jadavpur University (co-supervisor: Dr. Indranath Sengupta).

7. Dr. Sourav Sen Gupta received his PhD degree (Title: Analysis and Implementation of RC4 Stream Cipher) in Computer Science in the year 2014 from Indian Statistical Institute.

8. Mr. Shashwat Raizada received his PhD degree in Computer Science at Indian Statistical Institute (Title: Some results on the Analysis and Implementation of HC-128 Stream Cipher) in January 2015.

9. Mr. Subhadeep Banik received his PhD degree in Computer Science at Indian Statistical Institute (Title: Some Studies on Selected Stream Ciphers. Analysis, Fault Attack & Related Results) in April 2015.

10. Mr. Toshanlal Meenpal received his PhD degree in Engineering Sciences at Homi Bhaba National Institute, BARC Mumbai, (Title: Studies in Techniques for Image and Video Security) in September 2015. (co-supervisors: Prof. A. K. Bhattacharjee and Prof. R. Balasubramanian).

11. Supervised more than 20 students for M. Tech. (CS) dissertation at Indian Statistical Institute.

6.2 Courses taught at Indian Statistical Institute, Kolkata

30 courses in last 15 years at B. Stat, M. Stat and M. Tech. level in the area of Computer Science. Each course is of approximately 50 hours per semester.

6.3 Other Professional and Editorial Works

1. Served as program committee member for (partial list)
   - IACR Workshops: FSE 2012, 2013, 2014, 2017, 2018, Eurocrypt 2013, Asiacrypt 2013;
   - Indocrypt 2002;
   - Information Security, 8th International Conference, Singapore, ISC 2005;
   - 11th Australasian Conference on Information Security and Privacy, ACISP 2006;
   - The Third International Workshop on Signal Design and Its Applications in Communications, China, IWSDA 2007;
   - Information Security, 11th International Conference, Taiwan, ISC 2008.
2. Reviewed papers for many other leading cryptology conferences like Crypto, Eurocrypt, Asiacrypt, SAC, FSE etc.
3. Journal paper review (partial list):
   IEEE Transactions on Information Theory,
   Journal of Cryptology,
   IEEE Transactions on Multimedia,
   Designs Codes and Cryptography,
   Theoretical Computer Science,
   Discrete Applied Mathematics,
   Discrete Mathematics,
   Information Processing Letters,
   Applicable Algebra in Engineering Communication and Computing.

6.4 Design and Development of Computer Software

1. A library of functions to study the cryptographic and combinatorial properties of Boolean functions.
2. Tools for analysis and design of watermarking and steganographic schemes.
3. Tools for cryptanalysis of different stream ciphers.

These softwares were developed as part of different external projects.

6.5 Earlier Experiences as Computer Professional

Cumulative experience: 3 years.

6.5.1 At DAIS Infotech

Organization	Dais Infotech Pvt. Ltd.
Address	SDF Building, Module 223-226, Salt Lake, Calcutta, Pin: 700 091
Designation	Software Engineer
Duration	1st August, 1996 to 3rd April, 1997

Software Projects :

1. Communication Software for handshaking PCs (OS: WINDOWS'95) with back end Mainframe Systems using Windows Programming with VC++.
2. Internet based Shipping Management Software using CGI (in C) with INFORMIX as back end database.
3. Development of Web Tools (mainly search engine) using JAVA.

6.5.2 At CMC Limited

Organization	CMC Limited
Address	28, Camac Street, Calcutta, Pin: 700 016
Designation	Information Technology Engineer
Duration	1st June, 1992 to 31st July, 1994

Software and Hardware Maintenance and Installation at Railway Reservation System, Calcutta, Indian Statistical Institute, Calcutta, Gun and Shell Factory, Cossipore, and Calcutta State Transport Corporation, Belghoria.

Software Projects

1. Maintenance of Railway Reservation System. This is the nationwide railway reservation system in India. The software was developed in FORTRAN using VAX FORMS for screens. The operating system is VMS.
2. Communication Software for connecting VAX 8650 and VAXSTATION 2000 using C on VMS operating system.
3. Transport Management Software using COBOL on UNIX platform.