Anup Kumar Bhattacharya

Contact Information

Department of Computer Science & Engineering,
Indian Institute of Technology, Kharagpur
Pin - 721302

E-mail: bhattacharya.anup@gmail.com
anup@cse.iitkgp.ernet.in

Education

M.S (by Research) in Computer Science and Engineering (January 2009 – present)
Department of Computer Science and Engineering,
Indian Institute of Technology, Kharagpur, West Bengal
Thesis advisor: Dr. Dipanwita Roychaudhury and Dr. Abhijit Das
Current CGPA: *9.41/10*

B.Tech in Electronics and Telecommunication Engineering (July 2002 – June 2006)
Department of Electronics and Telecommunication Engineering,
Jadavpur University, West Bengal
CGPA: *8.88/10*

Awards/ Achievements

Secured **41st position (top 0.06%)** among 70000 students in West Bengal Joint Entrance Examination, 02

Scored 551 (98.6%) in Electronics & Telecommunication Engg. in **GATE, 2006**

Work Experience

Industrial Experience: Worked as a **technical consultant** at PricewaterhouseCoopers from July, 2006 to August, 2008 on an ERP software named **Navision**

Research Experience: Working as a **research consultant** in a project sponsored by General Motors, India from September, 2008 up till now

Research Projects

Masters Level
Computer Science & Engineering Department, IIT Kharagpur

- **Design and analysis of an efficient cryptosystem for safety messaging over vehicular networks**, General Motors (R&D), India. (Sep. 2008 - Dec. 2009)
- **Efficient implementation of cryptographic primitives**, General Motors (R&D), India. (Jan. 2010 - present) Pairing based cryptography is used nowadays to design different cryptographic protocols like signature generation and verification etc. In this work, we are concentrating on efficient implementation of pairing on super-singular elliptic curves defined over characteristic 2 & 3. We design and implement efficient arithmetic for characteristic 2 & 3 fields. We implement variants of addition, multiplication, square, square root and inverse routines for these finite fields. Using these routines, we implement a variant of pairing defined over super-singular curves named Eta pairing. In this work, we are also exploiting the architectural facilities like SIMD parallelism for faster implementation of pairing. We are comparing between horizontal and vertical parallelizations using SIMD intrinsics.
- *Project Supervisor:* Prof. Dipanwita Roychaudhury
- *Project Co-Supervisor:* Dr. Abhijit Das