Brief Resume

Education

PHD, Department of Computer Science and Engineering, Indian Institute of Technology, Kharagpur, 2012 - 2016.
Master of Science , School of Information Technology, Indian Institute of Technology, Kharagpur, 2009-2011 (CGPA 9.38).
Bachelor of Technology, Electronics and Communication Engineering, West Bengal University of Technology, 2002-2006 (CGPA 8.42).
Higher Secondary Education, South Point High School (2002), (78.7%).
Secondary Education, Holy Child Institute (2000) , (90.2%: Held rank 40 within the State and first in school)

- Overview of ongoing PHD Work:

  Storage and management in cloud services are of growing importance due to their cost-effective approaches in using large shared resources. However, with public access to the information in clouds, security is a very important issue. Confidentiality of data can be preserved by encrypting critical data before storing it in the cloud. However, bringing the data back and processing after decryption also leads to an overhead and outweighs the advantage of cloud computing. Homomorphic encryption which allows operations directly on the encrypted data is a solution to reduce this overhead. However, operations defined over fully homomorphic domain are very limited. With the advent of cloud computing, we intend to revisit age old problems of searching and sorting on fully homomorphic data. This research aims to propose the first approach to perform sorting on encrypted data. Our work further analyzes the performance of such operations and proposes different techniques to accelerate the sorting process. Further, we investigate feasibility of search operation on encrypted data in cloud. However there are several practical limitations of applying the fully homomorphic encryption (FHE) scheme to solve real life problems. Finally, our aim is to design the hardware for such FHE based operations with efficient FHE addition and multiplication blocks.

- Summary of Masters Thesis

  - Title of MS Thesis: *FPGA Implementation of Binary Edwards Curve Using Ternary Representation*

    Elliptic Curve Cryptography (ECC) has proved to be one of the main pillars in the domain of Public-Key Cryptography. Further, Edwards Curve adds a new paradigm to ECC in terms of speed and security to exceptional point attacks. This curve has been recently extended to Binary Edwards Curves (BEC) to enable efficient implementation in $GF(2^m)$ fields while harvesting the advantages of a unified and complete scalar point multiplication. In this work, an implementation of BEC processor for state-of-the-art $GF(2^{233})$ field is explained with an effort to better utilize the Look-Up Tables (LUTs) of the FPGA. The design further implements the ternary algorithm to increase efficiency of the design. To the best of our knowledge this is the first reported result on implementations of BEC on FPGA platform. Subsequently, an analysis of the BEC processor is reported with respect to the power profiles of the design along with a modified version of ternary algorithm. The power profile supports the unified property of the BEC design along with its completeness and proves the design to be resistant against simple power analysis. Finally, this architecture is extended to incorporate the implementation of another important point operation, point halving. The main objective of this part of the design is to ensure the reconfiguribility of the system so that it can be easily extended to support scalar multiplications through other algorithms with minimal hardware addition.

Employment

- Details of employment :
  - **Research Scientist** , Data Center Technologies (DCT), Data Storage Institute (DSI), Agency for Science, Technology and Research (A*STAR), 2016 to 2018.
  - Worked as **Post Doctoral Researcher**, ISI Kolkata.
  - Worked as **Senior Research Fellow** in the Department of Computer Science and Engineering, Indian Institute of Technology, Kharagpur in a project : Neucleodyne Pvt Ltd. Sponsored Project on FPGA implementation of homomorphic cryptographic processors (from July 2011 to June 2013).
  - Worked as a **Junior Research Fellow** in School of Information Technology, IIT Kharagpur in a sponsored project by DIT on FPGA implementation of cryptographic processors (from June 2009-June 2011).
  - **Industry experience :** Worked as a **Project Engineer** in Wipro Technologies (from June 2006-June 2009).

Publications

List of Publications of Ayantika Chatterjee

- **Conference Papers:**
  1. Ayantika Chatterjee, Indranil Sengupta, FPGA Implementation of Learning with error based cryptosystem, VLSI Design 2014. (*Poster presentation*)
  2. Ayantika Chatterjee, Manish Kaushal, Indranil Sengupta: Accelerating Sorting of Fully Homomorphic Encrypted Data. INDOCRYPT 2013, LNCS: $262-273$.
  3. Ayantika Chatterjee, Indranil Sengupta: High-Speed Unified Elliptic Curve Cryptosystem on FPGAs Using Binary Huff Curves. VDAT 2012: 243-251.
  4. Ayantika Chatterjee, Indranil Sengupta: FPGA Implementation of Extended Reconfigurable Binary Edwards Curve based Processor, ICNC, February 2012, IEEE, Maui, Hawaii, USA.
  5. Ayantika Chatterjee, Indranil Sengupta: FPGA implementation of binary Edwards curve using ternary representation. ACM Great Lakes Symposium on VLSI,2011. Lausanne, Switzerland.pp. $73-78$.
- **Journal Papers**
  1. Ayantika Chatterjee, Indranil SenGupta, Sorting of Fully Homomorphic Encrypted Cloud Data: Can Partitioning be eective?, IEEE Transactions on Services Computing, DOI: 10.1109/TSC.2017.2711018, 2017.
  2. Ayantika Chatterjee, Indranil SenGupta, Translating Algorithms to handle Fully Homomorphic Encrypted Data on the Cloud, IEEE Transactions on Cloud Computing, doi:10.1109/TCC.2015.2481416.
  3. Ayantika Chatterjee, Indranil Sengupta: Performance Modeling and Acceleration of Binary Edwards Curve Processor on FPGAs, International Journal of Electronics and Information Engineering, 2014.
  4. Ayantika Chatterjee, Indranil Sengupta: Design of a High Performance Binary Edwards Curve based Processor Secured Against Side Channel Analysis, Integration the VLSI Journal, Elsevier, 2011.

- **Book**
    1. Fully Homomorphic Encryption in Real World Applications, Ayantika Chatterjee and Khin MiMi Aung, Publisher: Springer. (Under Preparation)

References

Prof I. Sen Gupta, Professor, Dept of Computer Sc and Engg, IIT Kharagpur, India
Email: isg@iitkgp.ac.in

Dr. Khin Mi Mi Aung, Senior Scientist, Agency for Science, Technology and Research (A*STAR), Data Storage Institute (DSI) Data Center Technologies Division, Singapore.
Email: khinmimiaung@gmail.com