Arnab **Bag**

PH.D. RESEARCH SCHOLAR

Secured Embedded Architecture Laboratory, Department of Computer Science and Engineering, Indian Institute of Technology, Kharagpur, West Bengal, INDIA, 721302

☎ (+91) 84-3639-8090 | ✉ arnabbag@iitkgp.ac.in | amiarnabbolchi | in amiarnabbolchi | S amiarnabbolchi

Summary

Third year Ph.D. Research Scholar under the supervision of **Professor Debdeep Mukhopadhyay** in the Department of Computer Science and Engineering, Indian Institute of Technology, Kharagpur. Current research interests include Hardware Security, Cryptographic Implementations, Public Key Cryptography, Post Quantum Cryptography, VLSI Design, Quantum Computing and Cryptography.

Education

Indian Institute of Technology
Kharagpur, West Bengal, INDIA

DOCTOR OF PHILOSOPHY *July. 2017 -*

- Institute Research Fellow under the supervision of **Professor Debdeep Mukhopadhyay** of the Department of Computer Science and Engineering, Indian Institute of Technology, Kharagpur

Indian Institute of Technology
Kharagpur, West Bengal, INDIA

B.TECH. + M.TECH. DUAL DEGREE IN ELECTRONICS AND ELECTRICAL COMMUNICATION ENGINEERING *July. 2012 - April. 2017*

- Secured overall CGPA 8.23 upon degree completion.

Patha Bhavana, Visva Bharati Central University
Santiniketan, West Bengal, INDIA

PRE-DEGREE IN SCIENCE *July. 2010 - April. 2012*

- Secured overall 97.5% upon final exam evaluation.

Patha Bhavana, Visva Bharati Central University
Santiniketan, West Bengal, INDIA

SCHOOL FINAL *July. 2000 - April. 2010*

- Secured overall 90.5% upon final exam evaluation.

Internship

National Remote Sensing Centre, Indian Space Research Organization
Hyderabad, Telengana, INDIA

SUMMER RESEARCH INTERN *May. 2015 - April. 2015*

- Demodulator Design, specifically, design of custom PLL based clock recovery system.
- Hardware implementation of the clock recovery system.
- Technical visit to the data acquisition and analysis facility of ISRO at Sadhnagar, Hyderabad, Telengana.

Publications

2020	**Fault Template Attacks on Block Ciphers Exploiting Fault Propagation,** IACR Conference, Eurocrypt	*Zagreb, Croatia*
2019	**Enhancing Fault Tolerance of Neural Networks for Security-Critical Applications,** ACM-IEEE Conference Poster, Design and Automation Conference (DAC)	*Las Vegas, USA*
2020	**Compact and Flexible Tate Pairing Over Barreto-Naehrig Curve using Redundant Number System on FPGA,** (Under Review)	*,*
2018	**Hardware Acceleration for Searchable Encryption,** ACM SIGSAC Conference, ACM CCS Poster	*Toronto, Canada*
2018	**Cryptographically Secure Multi-Tenant Provisioning of FPGAs,** ACM-IEEE Conference Poster, Design and Automation Conference (DAC)	*Sun Francisco, USA*
2017	**A Review on Emotion Recognition using Speech,** IEEE conference ICICCT	*Coimbatore, INDIA*
2016	**Effects of Emotion on Physiological Signals,** IEEE conference INDICON	*Bengaluru, INDIA*
2015	**Affect Detection in Normal Groups with the Help of Biological Markers,** IEEE conference INDICON	*Delhi, INDIA*
2015	**Emotion Recognition Based on Physiological Signals using Valence-Arousal Model,** IEEE conference ICIIP	*Delhi, INDIA*

Projects

Secured Hardware Extension *Department of CSE, IIT Kharagpur*

SPONSORED PROJECT *May. 2017 - September. 2017*

- Developed the hardware implementation from scratch of an Automotive Secured Hardware Extension and tested on FPGA as a part of the project **LPI-1 : Formal Methods for Physical Security Verification of Cryptographic Designs against Fault Attacks**, sponsored by **Synopsys USA**, under the supervision of Professor Debdeep Mukhopadhyay and Professor Pallab Dasgupta, Department of Computer Science and Engineering, IIT Kharagpur

Book Chapter

Fault-Tolerant Implementations of Physically Unclonable Functions on FPGA *Springer Nature Switzerland AG*

SECURITY AND FAULT TOLERANCE IN INTERNET OF THINGS *2019*

Teaching Experience

2019,2020	**Teaching Assistant**, High Performance Computer Architecture - PG Level Course	*Department of CSE*
2019	**Teaching Assistant**, Cryptography and Network Security - PG Level Elective Course	*Department of CSE*
2018	**Teaching Assistant**, Computer Organization and Architecture - UG Level Laboratory Course	*Department of CSE*
2018	**Teaching Assistant**, Hardware Security - PG Level Elective Course	*Department of CSE*

Work Experience

Intugine Technologies *Kharagpur, India*

SOFTWARE DEVELOPER *August. 2014 - September. 2014*

- Worked as a software developer for two months in a startup company - Intugine Technologies, developed socket based communication and multi-threaded controller application for gesture control device.

Competitions

HACK@ DAC *DAC 2018 Hardware Security Contest, San Francisco, USA*

WINNER *April 2018*

- Member of the winning team of the Hardware Security competition held at Design Automation Conference 2018 in San Francisco, USA

Committees

2020	**IACR Student Member**,	*Kharagpur, INDIA*
2017	**IEEE Student Member**, IEEE Circuits and Systems Society	*Kharagpur, INDIA*

Skills

Core	**FPGA Based Design, ASIC Design**,
Dev. Boards	**VC707 Virtex-7, Basys-3, Nexsys-4, ZedBoard, Sasebo G, Sakura GII, Sakura GW, Sakura X**,
Tools	**Cadence Virtuoso, Synopsys Design Compiler, Synopsys IC Compiler, Synopsys Custom Designer, Xilinx Vivado**,
Languages	**Verilog, C++, Python, TCL**,