SANDIP KARMAKAR

20, Vidyasagar Road, Nabagram, Dist.-Hooghly, WB, India – 712246|sandip1kk@gmail.com|+919748042664

EDUCATION

Areas of Interest: Cryptology, Side Channel Attacks, Fault Attacks, Algebraic Attacks, Cellular Automata.

Indian Institute of Technology, Kharagpur, WB, India

Ph.D. in Computer Science and Engineering, Specialization: Cryptography **August 2014**
UNDER GUIDANCE OF: PROFESSOR DIPANWITA ROY CHOWDHURY.
THESIS: SIDE CHANNEL ATTACKS ON STREAM CIPHERS AND COUNTERMEASURES
COURSEWORK: ADVANCED GRAPH THEORY, ARTIFICIAL INTELLIGENCE, EMBEDDED SYSTEMS.

Indian Institute of Technology, Kharagpur, WB, India

MS (By Research) in Computer Science and Engineering, Specialization: Cryptography **October 2010**
UNDER GUIDANCE OF: PROFESSOR DIPANWITA ROY CHOWDHURY AND DR. DEBDEEP MUKHOPADHYAY.
THESIS: APPLICATION OF CELLULAR AUTOMATA IN DESIGN OF STREAM CIPHERS
COURSEWORK: CRYPTOGRAPHY & NETWORK SECURITY, FOUNDATIONS OF CRYPTOGRAPHY, ADVANCES IN ALGORITHMS, COMPUTATIONAL NUMBER THEORY, ENGLISH FOR TECHNICAL WRITING.

Bengal Engineering and Science University, Howrah, WB, India (Currently, IIEST, Shibpur)

BE in Computer Science and Technology **June 2004**

EXPERIENCE

TEACHING EXPERIENCE

INDIAN INSTITUTE OF INFORMATION TECHNOLOGY, KALYANI, WB,

Assistant Professor,

July 2016 – till date

Subjects Taught:
Digital Logic and Circuit Design (July 2016 – November 2016)
Database Management Systems [Theory] (July 2016 – November 2016)
Database Management Systems [Lab] (July 2016 – November 2016)
Algorithms (Jan 2017-till date)
Compiler Design (Jan 2017-till date)
Compiler Design Lab (Jan 2017-till date)

INDIAN INSTITUTE OF INFORMATION TECHNOLOGY, GUWAHATI, ASSAM,

Assistant Professor,

July 2014 – June 2016

Subjects Taught:
Algorithms (July 2014 – November 2014)
Database Management Systems [Theory] (Jan 2015 – April 2015)
Database Management Systems [Lab] (Jan 2015 – April 2015)
Theory of Computation (July 2015 – November 2015)
Formal Languages and Automata Theory (January 2016- April 2016)
Topics in Algorithms (Parallel Algorithms) (January 2016- April 2016)

Student Guidance:
B.Tech. – 2nd Year Project – 12 Students
B.Tech. – 3rd Year Project – 5 Students

Course Design:
Parallel Algorithms (December 2015)

INDIAN INSTITUTE OF TECHNOLOGY KHARAGPUR, KHARAGPUR, WB

Teaching Assistantships **July 2008-Dec 2013**
Computer Architecture Lab (Aug. 2008 - Nov.2008)
Switching Circuit Lab (Jan.2009 - May.2009)
Cryptography & Network Security [Theory] (Aug.2009 - Nov.2009)
Foundations of Cryptography [Theory] (Jan.2010 - May.2010)
Programming & Data Structures [Theory] (Aug.2010 - Nov.2010)
Operating Systems Lab (Jan.2011 – May 2011)
Cryptography & Network Security [Theory] (Aug. 2011 – Nov. 2011)
Programming & Data Structure Lab (Jan.2012 – May 2012)
Cryptography and Network Security [Theory] (Jul 2012 – Nov 2012)
Foundations of Cryptography [Theory] (Jan 2013 – April 2013)
Programming & Data Structure [Lab] (Aug. 2013-Nov 2013)

RESEARCH PROJECT EXPERIENCE

SRIC, IIT Kharagpur, Kharagpur, WB,
Indian Telephone Industry, Bangalore
Research Consultant **May 2008-December 2010**
Design and Implementation of an Indigenous Encryption System
(FPGA implementation, Language-Verilog)

SRIC, IIT Kharagpur, Kharagpur, WB,
Scientific Analysis Group, DRDO, Delhi
Senior Scientific Officer **January 2011 – August 2012**
Software Tools for Cryptanalysis of Stream Ciphers
(Implemented Cube Attack, Language-C)

INDUSTRIAL EXPERIENCE

TATA Consultancy Services
Assistant Systems Engineer **November 2006 – December 2007**
Development of Java/J2ee based web-projects in *financial domain*

TCG Software Services Pvt. Ltd.
Software Engineer **July 2004 – August 2006**
Development of Java/J2ee based web-projects in *banking domain*

PUBLICATIONS AND PAPERS

JOURNALS

1. **Sandip Karmakar**, Debdeep Mukhopadhyay and Dipanwita Roy Chowdhury. CAvium – Strengthening Trivium using Cellular Automata. Journal of Cellular Automata 7(2) 179-197. 2012. (SCOPUS/SCI) (During PhD).

2. **Sandip Karmakar** and Dipanwita Roy Chowdhury. Leakage Squeezing using Cellular Automata and its Application to Scan Attack. J. Cellular Automata 9(5-6): 417-436 (2014). (SCOPUS/SCI) (During PhD).

3. **Sandip Karmakar** and Dipanwita Roy Chowdhury. Design and Analysis of Some Non-uniform Nonlinear Cryptographically Robust Cellular Automata. Journal of Cellular Automata. (to appear) (SCOPUS/SCI) (Post-PhD).

CONFERENCES

1. **Sandip Karmakar** and Dipanwita Roy Chowdhury. Differential Fault Analysis of MICKEY-128 2.0. IEEE FDTC 2013. 52-59, Santa Barbara, CA, USA, 20th August, 2013. CORE RANK – C.

2. **Sandip Karmakar** and Dipanwita Roy Chowdhury. Leakage Squeezing using Cellular Automata. Gieben, Germany, Automata 2013,98-109. Giessen, Germany, September 2013.CORE Ranking-Not Available. ***(Presented)***

3. **Sandip Karmakar** and Dipanwita Roy Chowdhury. Countermeasures of Side Channel Attacks on Symmetric Key Ciphers using Cellular Automata. ACRI 2012.623-632, Santorini, Greece. CORE Ranking-Not Available.

4. **Sandip Karmakar** and Dipanwita Roy Chowdhury. NOCAS: A Nonlinear Cellular Automata Based Stream Cipher. Automata 2011, 17th International Workshop on Cellular Automata and Discrete Complex Systems,135-146. November 21-23, 2011, Santiago, Chile. CORE Ranking-Not Available.

5. **Sandip Karmakar** and Dipanwita Roy Chowdhury. Fault Analysis of Grain-128 by Targeting NFSR. Africacrypt 2011, 298-315, July 5-7, 2011, Dakar, Senegal. CORE Ranking-Not Available.

6. Mukesh Agrawal, **Sandip Karmakar**, Dhiman Saha and Debdeep Mukhopadhayay. Scan Based Side Channel Attacks on Stream Ciphers and their Counter-measures. Progress in Cryptology - INDOCRYPT 2008, Volume 5365/2008, pages 226-238, December 2008, Kharagpur, India. CORE Ranking-B.

7. **Sandip Karmakar**, Debdeep Mukhopadhyay and Dipanwita Roy Chowdhury. d-monomial Tests on Nonlinear Cellular Automata for Cryptographic Design. ACRI 2010,261-270. Ascoli Piceno, Italy, September 2010. CORE Ranking-Not Available.

8. **Sandip Karmakar**, Debdeep Mukhopadhyay and Dipanwita Roy Chowdhury. CAvium - Strengthening Trivium using Cellular Automata. (Short Paper) Automata 2010, Nancy, France, June 2010. CORE Ranking-Not Available.

9. **Sandip Karmakar**, Debdeep Mukhopadhyay and Dipanwita Roy Chowdhury. Cube Attack on a Simplified version of Trivium. National Workshop of Cryptology 2010, Coimbatore, India. CORE Ranking-Not Available. ***(Presented)***

10. **Sandip Karmakar**, Debdeep Mukhopadhyay and Dipanwita Roy Chowdhury. A New Cellular Automata Ruleset for Cryptographic Pseudorandom Sequence Generation. National Workshop of Cryptology 2009, SVNIT, Surat, India. CORE Ranking-Not Available. ***(Presented)***

11. Dhiman Saha, **Sandip Karmakar**, Debdeep Mukhopadhyay and Dipanwita Roy Chowdhury. An FPGA implementation of the Trivium Stream Cipher. National Workshop of Cryptology 2008, Hyderabad, India. CORE Ranking-Not Available.

---END---