Sk. Subidh Ali

Contact Information

Department of Computer Science and Engineering
Indian Institute of Technology Kharagpur
Kharagpur
West Bengal
India

Phone: +91-3222-282255
Fax: +91-3222-278985
*Email:*subidh@cse.iitkgp.ernet.in
*WWW:*http://iitkgp.ac.in

- More information and auxiliary documents can be found at `http://cse.iitkgp.ac.in/ ska/`

Research Interests

Side-channel attacks, design of fault tolerant crypto-systems, fault based cryptanalysis, high speed cryptography, mobile computing.

Education

Indian Institute of Technology, Kharagpur, India

Ph.D.(Pursuing), Computer Science and Engineering,

- Thesis Topic: *Design and Analysis of Fault Tolerant Crypto-systems*
- Advisor: Professor Debdeep Mukhopadhyay
- Area of Study: Cryptography

M.E., West Bengal University of Technology,Kolkata
Information Technology, December 2007

- Thesis Topic: *Design and Analysis of Ad-hoc Routing Protocols*
- Area of Study: Mobile Computing

B.E., Bankura Unnayani Institute of Engineering
Computer Science and Engineering, June 2003

Conference Publications

Sk. Subidh Ali, and Debdeep Mukhopadhyay, "An Improved Differential Fault Analysis on AES-256", To Appear in the Proceedings of AfricaCrypt 2011, Senegal.

Sk. Subidh Ali, Rajat Subhra Chakraborty, Debdeep Mukhopadhyay and Swarup Bhunia, "Multi-level Attack: an Emerging Threat Model for Cryptographic Hardware", To Appear in the Proceedings of DATE 2011, France.

Michael Tunstall, Debdeep Mukhopadhyay, and **Sk. Subidh Ali**, "Differential Fault Analysis of the Advanced Encryption Standard using a Single Fault", To Appear in the Proceedings of WISTP 2011, Greece.

Sk. Subidh Ali, Debdeep Mukhopadhyay, and Michael Tunstall. "Differential Fault Analysis of AES using a Single Multiple-Byte Fault." Cryptology ePrint Archive: Report 2010/636.

Sk. Subidh Ali and Debdeep Mukhopadhyay. "Acceleration of Differential Fault Analysis of the Advanced Encryption Standard Using Single Fault." Cryptology ePrint Archive: Report 2010/451.

Sk. Subidh Ali, C. Rebeiro, and D. Mukhopadhyay, "Cache Aware Tools for Cryptographic Applications", in the National Workshop on Cryptology, 2009

Awards

MHRD scholarship at IIT Kharagpur for P.hD programme (2009-2012)

Teaching Experience

Teaching Assistant Computer Science and Engineering
IIT, Kharagpur

- (Programming and Data Structure Lab.) **January 2009 to April 2009**
- (Computer Network and Operating System Lab. **July 2009 to December 2009**
- (Programming and Data Structure Lab) **January 2010 to April 2010**
- (Programming and Data Structure Lab) **July 2010 to December 2010**
- (Programming and Data Structure Lab) **January 2011 to April 2011**

Lecturer Bankura Unnayani Institute of Engineering
Computer Science and Engineering, January 2007-December 2008

Lecturer Bankura Unnayani Institute of Engineering
Computer Science and Engineering, August 2004-December 2005

Lecturer Central Calcutta Polytechnic Kolkata
Computer Science and Engineering, September 2003-August 2004

References Available to Contact

Dr. Debdeep Mukhopadhyay (e-mail: debdeep@cse.iitkgp.ernet.in; phone: +91-3222-282255)
Assistant Professor,
Computer Science and Engineering,
Indian Institute of Technology Kharagpur