

Sr No	Paper title and Authors
1.	<p><b>Differential Power Attack On FPGA Implementation of Triple-DES</b>  Dhiman Saha<sup>1</sup>, Debdeep Mukhopadhyay<sup>2</sup>, Dipanwita Roy Chowdhury<sup>3</sup>  <sup>1</sup>MS Student, Dept. of Computer Science and Engineering, Indian Institute of Technology, Kharagpur, West Bengal 721-302  <sup>2</sup>Assistant Professor, Dept. of Computer Science and Engineering, Indian Institute of Technology, Kharagpur, West Bengal 721-302  <sup>3</sup>Professor, Dept. of Computer Science and Engineering, Indian Institute of Technology Kharagpur, West Bengal 721-302  <sup>1</sup><a href="mailto:saha.dhiman@gmail.com">saha.dhiman@gmail.com</a>, <sup>2</sup><a href="mailto:debdeep.mukhopadhyay@gmail.com">debdeep.mukhopadhyay@gmail.com</a>, <sup>3</sup><a href="mailto:drc@cse.iitkgp.ernet.in">drc@cse.iitkgp.ernet.in</a></p>
2.	<p><b>An Ideal Multi-Secret Sharing Scheme for General Access Structure</b>  Partha Sarathi Roy<sup>1</sup>, Avishek Adhikari<sup>2</sup>  <sup>1,2</sup>Department of Pure Mathematics, University of Calcutta, 35 Ballygunge Circular Road, Kolkata - 700 019, West Bengal, India  <sup>1</sup><a href="mailto:royparthasarathi0@gmail.com">royparthasarathi0@gmail.com</a>, <sup>2</sup><a href="mailto:aamath@caluniv.ac.in">aamath@caluniv.ac.in</a></p>
3.	<p><b>An efficient multi-secret sharing scheme</b>  Angsuman Das<sup>1</sup>, Avishek Adhikari<sup>2</sup>  <sup>1,2</sup>Department of Pure Mathematics, University of Calcutta, Kolkata, India  <sup>1</sup><a href="mailto:angsumandas054@gmail.com">angsumandas054@gmail.com</a>, <sup>2</sup><a href="mailto:aamath@caluniv.ac.in">aamath@caluniv.ac.in</a></p>
4.	<p><b>NSA Suit-B ECMQV Key Agreement Protocol on FPGA Platform</b>  Santosh Ghosh<sup>1</sup>, Dipanwita Roy Chowdhury<sup>2</sup>, Indranil Sen Gupta<sup>3</sup>  <sup>1,2,3</sup>Dept. of Computer Sc. &amp; Engg., Indian Institute of Technology Kharagpur, WB, India, 721302  <sup>1</sup><a href="mailto:santosh@cse.iitkgp.ernet.in">santosh@cse.iitkgp.ernet.in</a>, <sup>2</sup><a href="mailto:drc@cse.iitkgp.ernet.in">drc@cse.iitkgp.ernet.in</a>, <sup>3</sup><a href="mailto:isg@cse.iitkgp.ernet.in">isg@cse.iitkgp.ernet.in</a></p>
5.	<p><b>On Resiliency of Orthogonal Array based Key Predistribution Scheme</b>  Anupam Pattanayak<sup>1</sup>, Banshidhar Majhi<sup>2</sup>  <sup>1,2</sup>Computer Science &amp; Engineering Department National Institute of Technology Rourkela Rourkela, India  <sup>1</sup><a href="mailto:anupam.pk@gmail.com">anupam.pk@gmail.com</a>, <sup>2</sup><a href="mailto:bmajhi@nitrkl.ac.in">bmajhi@nitrkl.ac.in</a></p>
6.	<p><b>A Rabin Type Scheme Based on Singular Cubic Curve</b>  Sahadeo Padhye<sup>1</sup>  <sup>1</sup>Department of Mathematics Motilal Nehru National Institute of Technology, Allahabad(UP), India  <sup>1</sup><a href="mailto:sahadeo@mnnit.ac.in">sahadeo@mnnit.ac.in</a>, <sup>1</sup><a href="mailto:sahadeo_mathrsu@yahoo.com">sahadeo_mathrsu@yahoo.com</a></p>
7.	<p><b>New Non Linear Stream Cipher based on Cellular Automata</b>  Debabrata Dey<sup>1</sup>, Dipanwita Roy Chowdhury<sup>2</sup>  <sup>1,2</sup>Computer Science &amp; Engineering Department, Indian Institute of Technology, I.I.T KGP, Kharagpur, West Bengal, India  <sup>1</sup><a href="mailto:debu@cse.iitkgp.ernet.in">debu@cse.iitkgp.ernet.in</a>, <sup>2</sup><a href="mailto:drc@cse.iitkgp.ernet.in">drc@cse.iitkgp.ernet.in</a></p>
8.	<p><b>A 4-Character Stream Ciphery Technique by Random Key Substitution: A Concept of Hardware Implementation</b>  Joydip Dutta<sup>1</sup>, Shankhadeep Karmakar<sup>2</sup>, Bikash Patra<sup>3</sup>, J K M Sadique Uz Zaman<sup>4</sup>, Ranjan Ghosh<sup>5</sup>  <sup>1,2,3</sup>B. Tech Students of Information Technology, Institute of Radio Physics and Electronics, University of Calcutta, 92, Acharya Prafulla Chandra Road, Kolkata - 700 009  <sup>4</sup>Junior Research Fellow(RFSMS), Institute of Radio Physics and Electronics, University of Calcutta, 92, Acharya Prafulla Chandra Road, Kolkata - 700 009  <sup>5</sup>Institute of Radio Physics and Electronics, University of Calcutta, 92, Acharya Prafulla Chandra Road, Kolkata - 700 009  <sup>5</sup><a href="mailto:rghosh47@gmail.com">rghosh47@gmail.com</a></p>

9.	<p><b>Smix: A New Highly Non-linear Reversible Boolean Function</b></p> <p>Jaydeb Bhaumik<sup>1</sup>, Debdeep Mukhopadhyay<sup>2</sup>, Dipanwita Roy Chowdhury<sup>3</sup>  <sup>1</sup><i>G. S. Sanyal School of Telecommunications, Indian Institute of Technology, Kharagpur</i>  <sup>2,3</sup><i>Dept. of Computer Science &amp; Engg, Indian Institute of Technology, Kharagpur</i>  <sup>1</sup><a href="mailto:jaydeb@gssst.iitkgp.ernet.in">jaydeb@gssst.iitkgp.ernet.in</a>, <sup>2</sup><a href="mailto:debdeep@cse.iitkgp.ernet.in">debdeep@cse.iitkgp.ernet.in</a>, <sup>3</sup><a href="mailto:drc@cse.iitkgp.ernet.in">drc@cse.iitkgp.ernet.in</a></p>
10.	<p><b>Group Signature Scheme using CRT</b></p> <p>Anup Kumar Bhattacharya<sup>1</sup>, Abhijit Das<sup>2</sup>, Dipanwita Roy Choudhuri<sup>3</sup>, Umang Jain<sup>4</sup>, Nitin Bansal<sup>5</sup>  <sup>1,2,3,4,5</sup><i>Department of Computer Science &amp; Engineering, IIT Kharagpur</i>  <sup>1</sup><a href="mailto:fanup@cse.iitkgp.ernet.in">fanup@cse.iitkgp.ernet.in</a>, <sup>2</sup><a href="mailto:abhij@cse.iitkgp.ernet.in">abhij@cse.iitkgp.ernet.in</a>, <sup>3</sup><a href="mailto:drcg@cse.iitkgp.ernet.in">drcg@cse.iitkgp.ernet.in</a></p>
11.	<p><b>A New Cellular Automata Ruleset for Cryptographic Pseudorandom Sequence Generation</b></p> <p>Sandip Karmakar<sup>1</sup>, Debdeep Mukhopadhyay<sup>2</sup>, Dipanwita Roy Chowdhury<sup>3</sup>  <sup>1</sup><i>MS Student, Indian Institute of Technology, Kharagpur</i>  <sup>2,3</sup><i>Dept. of Computer Science &amp; Engg, Indian Institute of Technology, Kharagpur</i>  <sup>1</sup><a href="mailto:sandip.2179@yahoo.com">sandip.2179@yahoo.com</a>, <sup>2</sup><a href="mailto:debdeep@cse.iitkgp.ernet.in">debdeep@cse.iitkgp.ernet.in</a>, <sup>3</sup><a href="mailto:drc@cse.iitkgp.ernet.in">drc@cse.iitkgp.ernet.in</a></p>
12.	<p><b>Cache Aware Tools for Cryptographic Applications</b></p> <p>Sk. Subidh Ali<sup>1</sup>, Chester Rebeiro<sup>2</sup>, Debdeep Mukhopadhyay<sup>3</sup>  <sup>1,2,3</sup><i>Dept. of Computer Science and Engineering, IIT Kharagpur, India</i>  <sup>1</sup><a href="mailto:subidh@gmail.com">subidh@gmail.com</a>, <sup>2</sup><a href="mailto:rebeiro@gmail.com">rebeiro@gmail.com</a>, <sup>3</sup><a href="mailto:debdeep@cse.iitkgp.ernet.in">debdeep@cse.iitkgp.ernet.in</a></p>
13.	<p><b>(2; n)-Visual Cryptographic Schemes For Color Images With Low Pixel Expansion</b></p> <p>Bhaswar B. Bhattacharya<sup>1</sup>, Abhishek Chakraborty<sup>2</sup>, Shirshendu Ganguly<sup>3</sup>, Shyamalendu Sinha<sup>4</sup>  <sup>1,2,3,4</sup><i>Indian Statistical Institute, Kolkata - 700 108, India</i>  <sup>1</sup><a href="mailto:bhaswar.bhattacharya@gmail.com">bhaswar.bhattacharya@gmail.com</a></p>
14.	<p><b>On a Modification of Solovay-Strassen Test for Primality</b></p> <p>Souvik Meta<sup>1</sup>, Sujayendu Patra<sup>2</sup>, Sayan Das<sup>3</sup>, Subhajit Goswami<sup>4</sup>  <sup>1,2,3,4</sup><i>Indian Statistical Institute, Kolkata - 700 108, India</i>  <sup>4</sup><a href="mailto:cal.subhajit@gmail.com">cal.subhajit@gmail.com</a></p>
15.	<p><b>Approaches to Formal Verification of Security Protocols</b></p> <p>Suvansh Lal<sup>1</sup>, Mohit Jain<sup>2</sup>, Vikrant Chaplot<sup>3</sup>  <sup>1,2,3</sup><i>B. Tech Students, Dhirubhai Ambani Institute of Information and Communication Technology, Gandhinagar, Gujarat, India</i>  <sup>1</sup><a href="mailto:suvansh_lal@daiict.ac.in">suvansh_lal@daiict.ac.in</a>, <sup>2</sup><a href="mailto:miohit_jain@daiict.ac.in">miohit_jain@daiict.ac.in</a>, <sup>3</sup><a href="mailto:vikrant_chaplot@daiict.ac.in">vikrant_chaplot@daiict.ac.in</a></p>
16.	<p><b>Addressing BGP Vulnerabilities Using External Security Monitoring Schemes</b></p> <p>Hiren B. Patel<sup>1</sup>, Dr. Dhiren R. Patel<sup>2</sup>  <sup>1</sup><i>Department of Computer Engineering, S. P. College of Engineering, Visnagar, India - 384315</i>  <sup>2</sup><i>Department of Computer Engineering, S.V.National Institute of Technology, Surat, India - 395007</i>  <sup>1</sup><a href="mailto:hbpatel1976@yahoo.com">hbpatel1976@yahoo.com</a>, <sup>2</sup><a href="mailto:dhiren29p@gmail.com">dhiren29p@gmail.com</a></p>
17.	<p><b>Attacks on Computer Networks: Motivation to Design Attack Resilient MAC Protocol</b></p> <p>Piyush Kumar Shukla<sup>1</sup>, S. Silakari<sup>2</sup>, S.S. Bhadouria<sup>3</sup>  <sup>1,2</sup><i>Dept. of CSE, UIT, RGPV, Bhopal, M.P., INDIA</i>  <sup>3</sup><i>Dept. of EC, MITS, Gwalior</i>  <sup>1</sup><a href="mailto:pphdw@yahoo.com">pphdw@yahoo.com</a>, <sup>2</sup><a href="mailto:sslakari@yahoo.com">sslakari@yahoo.com</a>, <sup>3</sup><a href="mailto:Saitamts61@yahoo.co.in">Saitamts61@yahoo.co.in</a></p>