2020 Third ISEA Conference on Security and Privacy (ISEA-ISAP 2020)

Guwahati, India
27 February – 1 March 2020

IEEE Catalog Number: CFP20K78-POD
ISBN: 978-1-7281-6709-1

Copyright © 2020 by the Institute of Electrical and Electronics Engineers, Inc.
All Rights Reserved

Copyright and Reprint Permissions: Abstracting is permitted with credit to the source. Libraries are permitted to photocopy beyond the limit of U.S. copyright law for private use of patrons those articles in this volume that carry a code at the bottom of the first page, provided the per-copy fee indicated in the code is paid through Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923.

For other copying, reprint or republication permission, write to IEEE Copyrights Manager, IEEE Service Center, 445 Hoes Lane, Piscataway, NJ 08854. All rights reserved.

****** This is a print representation of what appears in the IEEE Digital Library. Some format issues inherent in the e-media version may also appear in this print version.***

IEEE Catalog Number:	CFP20K78-POD
ISBN (Print-On-Demand):	978-1-7281-6709-1
ISBN (Online):	978-1-7281-6708-4

Additional Copies of This Publication Are Available From:

Curran Associates, Inc
57 Morehouse Lane
Red Hook, NY 12571 USA
Phone: (845) 758-0400
Fax: (845) 758-2633
E-mail: curran@proceedings.com
Web: www.proceedings.com

Contents

1 Investigating Elliptic Curve Cryptography for Securing Smart Grid Environments 1

2 Security Notions for the VERAGREG Framework and Their Reductions 8

3 XSSD: A Cross-site Scripting Attack Dataset and its Evaluation 21

4 A Parallel Quad Itoh-Tsujii Multiplicative Inversion Algorithm for FPGA Platforms 31

5 DeDOP: Deduplication with cross-server Ownership over encrypted data 36

6 Detection of DDoS Attack and Classification Using a Hybrid Approach 41

7 Implementation of Minimally Shared Blockchains using Big Data Applications 48

8 Enhanced Anonymity: Customized for Roaming and Non-Roaming IoT-Devices in 5G Mobile Network 55

9 A LDPC codes based Authentication Scheme 63

10 An Approach to Identify Vulnerable Features of Instant Messenger 71

11 A Traffic Monitoring and Policy Enforcement Framework for HTTP 81

12 Enhancing Privacy in a Blockchain-based Public Key Infrastructure 87

13 Secure transmission of Hyperspectral Images 94

14 Provisioning Privacy and Accountability in Participatory Sensing 100

15 On the DSA Key Recovery Attack with Variable Partial Nonces Known 106

16 Implementation of AES Using Composite Field Arithmetic for IoT Applications 115

17 Security Testbed for Next Generation Mobile Networks 122

18 A Secured Land Registration Framework on Blockchain 130

19 Singleton Flow Traceback (SFT) Mechanism 139

20 2SPUF: Machine Learning Attack Resistant SRAM PUF 149

21 An Approach Towards Resisting Side-Channel Attacks for Secured Testing of Advanced Encryption Algorithm (AES) Cryptochip 155

22 Graph Convolutional Networks for Android Malware Detection with System Call Graphs 162

23 Inter-Planetary File System Enabled Blockchain Solution For Securing Healthcare Records 171