

2022 IEEE International Conference on Public Key Infrastructure and its Applications (PKIA 2022)

**Bangalore, India
9-10 September 2022**



**IEEE Catalog Number: CFP22N53-POD
ISBN: 978-1-6654-8884-6**

**Copyright © 2022 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:	CFP22N53-POD
ISBN (Print-On-Demand):	978-1-6654-8884-6
ISBN (Online):	978-1-6654-8883-9

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

CURRAN ASSOCIATES INC.
proceedings
.com

TABLE OF CONTENTS

Security Analysis of LDPC Code-Based Encryption	1
<i>Dibyasree Guha, Debasish Bera, Sourabh Biswas</i>	
Experimentation on Usage of PQC Algorithms for eSign.....	8
<i>Pavan Kurariya, Ankita Bhargava, Srikanth Sailada, N. Subramanian, Jahnavi Bodhankar, Ajai Kumar</i>	
A Hybrid Hyperchaotic Based Dynamic Keystream Generator using Perturbance Process for Public Key Infrastructure Application.....	14
<i>Anirudh M Sivapriya, Dilip Kumar Barman, K. K. Soundra Pandian</i>	
Random Number Generation for PKI using Controlled Anderson PUF	20
<i>Aditi Roy, J Kokila, N Ramasubramanian, Shameedha B. Begum</i>	
Unconfirmed Transactions in Cryptocurrency: Reasons, Statistics, and Mitigation	26
<i>Harshal Shridhar Kallurkar, B R Chandavarkar</i>	
FPGA Based High Throughput Substitution Box Architectures for Lightweight Block Ciphers	33
<i>Ruby Mishra, Manish Okade, Kamalakanta Mahapatra</i>	
Public Key Cryptographic Implementation Validation: A Review	40
<i>P. V. Ananda Mohan, Abey Jacob, Raghavendra S. Patil</i>	
A Study of PKI Ecosystem in South Asian and Oceania Countries	48
<i>Lavanya Palani, Anoop Kumar Pandey, Balaji Rajendran, B S Bindhumadhava, S D Sudarsan</i>	
Identity of Things (IDoT): A Preliminary Report on Identity Management Solutions for IoT Devices	53
<i>Mohammed Misbahuddin, Rashmi Harish, K Ananya</i>	
Radian: Leveraging PKI for Long-Term Validation Enabled Digital Academic Testimonials - A Case-Study.....	62
<i>Souvik Pan, Dhiman Saha, Rajat Moona</i>	
Improved PKI Certificate Lifecycle Management with Centralized Device Management for Industrial IoT.....	70
<i>Ashwin A Krishnan, Satish Kumar Rajendran, T K Sunil Kumar</i>	
PKI for IoT using the DNS Infrastructure	75
<i>Sandoche Balakrichenan, Ibrahim Ayoub, Benoît Ampeau</i>	
A JSON Web Signature Based Adaptive Authentication Modality for Healthcare Applications	83
<i>Vivin Krishnan, C S Sreeja, Sumitra Binu, Mohammed Misbahuddin</i>	
Towards Automated PKI Trust Transfer for IoT.....	91
<i>Joel Höglund, Shahid Raza, Martin Furuhed</i>	
Evolving Role of PKI in Facilitating Trust.....	99
<i>Vishwas T. Patil, R. K. Shyamasundar</i>	

Author Index