

2023 16th International Conference on Information Security and Cryptology (ISCTurkiye 2023)

**Ankara, Turkey
18-19 October 2023**



**IEEE Catalog Number: CFP23AA5-POD
ISBN: 979-8-3503-9400-9**

**Copyright © 2023 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:	CFP23AA5-POD
ISBN (Print-On-Demand):	979-8-3503-9400-9
ISBN (Online):	979-8-3503-9399-6

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



www.iscturkey.org

16TH INTERNATIONAL CONFERENCE ON INFORMATION SECURITY AND CRYPTOLOGY

16. ULUSLARARASI BİLGİ GÜVENLİĞİ VE
KRİPTOLOJİ KONFERANSI

TABLE OF CONTENTS İÇİNDEKİLER

ID	eCF Paper ID	Paper Title	Authors	Pages
1	596008	Developing Explainable Intrusion Detection Systems for Internet of Things	Ahmet Furkan Çelik (Gazi University); Bedirhan Sağlam (Gazi University); Sedef Demirci (Gazi University)*	1-6
2	596023	Implementation of IP Multicast Network Specific Attacks on GNS3	Göksel Uçtu (Gazi University)*; Mustafa Alkan (Gazi Üniversitesi)	7-12
3	596010	POXIEM: An ELK Integrated SDN Controller Proposal for Improved Control Plane Forensic Visibility and Incident Response	Mevlut Serkan Tok (Gazi University)*; Mehmet Demirci (Gazi University)	13-18
4	596011	Adaptation of n-out-of-n secret sharing scheme into IoT network	Tuğberk Kocatekin (Istanbul Arel University)*; Cafer Çalışkan (Antalya Bilim University)	19-24
5	596012	TBNS: A Novel Tool for Simulating and Analyzing Bursty User Requests in Large-scale Networks	Ahmet Şanslı (Sakarya Üniversitesi)*; Tuğrul Taşçı (Sakarya Üniversitesi)	25-29
6	596013	Faster Secure Matrix Multiplication with the BGV Algorithm	Dilek Öner Şimşek (ODTÜ)*; Murat Cenk (ODTÜ)	30-34
7	596014	Security through Digital Twin-Based Intrusion Detection: A SWaT Dataset Analysis	Mehmet Bozdal (Abdullah Gül Üniversitesi)*	35-40
8	596015	A Blockchain Based Decentralized Identity, Access Management, and Trust Evaluation Framework for IoT	Buğrahan Saim Öztürk (ASELSAN)*; Murat Aydos (Hacettepe University)	41-46
9	596016	An Unrolled and Pipelined Architecture for SHA2 Family of Hash Functions on FPGA	Onur B Gamgam (Aselsan)*	47-52
10	596017	Differential and Linear Cryptanalysis of IVLBC via MILP Modeling	Murat burhan İLTER (Middle East Technical University, Aselsan Inc.)*;	53-57



www.iscturkey.org

16TH INTERNATIONAL CONFERENCE ON INFORMATION SECURITY AND CRYPTOLOGY

16. ULUSLARARASI BİLGİ GÜVENLİĞİ VE
KRİPTOLOJİ KONFERANSI

			Ali Aydın SELÇUK (TOBB ETÜ/TOBB University of Economics and Technology)	
11	596018	Comparison of ML-based One-Stage and Two-Stage NIDS Models	ONUR FIRAT ÖZTÜRK (Tetra Bilişim)*; Kazım Yıldız (Marmara University)	58-63
12	596019	QRAuth: A Secure and Accessible Web Authentication Alternative to FIDO2	Ahmet Drobi (Istanbul Technical University)*; Kemal Bicakci (Istanbul Technical University)	64-70
13	596020	Methods for Masking CRYSTALS-Kyber Against Side-Channel Attacks	Sıla Özeren (METU)*; Oğuz Yayla (METU)	71-76
14	596021	Comparison of Top 10 Well-Known Blockchain Consensus Algorithms	Hasan OZKUL (Hacettepe University)*; Enes Çeliker (Hacettepe University); Murat AYDOS (Hacettepe University); Adnan Özsoy (Hacettepe Üniversitesi)	77-82
15	596022	Mel Spektogram ile Ses Sahteciliği Tespiti Yöntemi - Audio Forgery Detection Method with Mel Spectrogram	Hatice Kübra GÜÇ (Karadeniz Teknik Üniversitesi)*; Beste USTUBİOĞLU (Karadeniz Technical University); Arda ÜSTÜBİOĞLU (Trabzon Üniversitesi); Güzin ULUTAŞ (Karadeniz Teknik Üniversitesi)	83-88
16	596009	Towards More Secure Virtual Reality Authentication for the Metaverse: A Decentralized Method Proposal	Pınar Kürtünlüoğlu (Muğla Sıtkı Koçman University); Beste Akdik (Muğla Sıtkı Koçman University); Reyhan Duygu (Muğla Sıtkı Koçman University); Enis Karaarslan (Muğla Sıtkı Koçman University)*	89-94