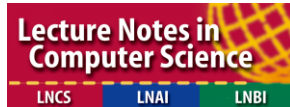




Springer



SCHEDULE
of
SECITC 2021: The 14th International Conference on Security for
Information Technology and Communications

25th-26th November 2021



Powered by



Informatics Security / IT&C Security
Master

Bucharest University of Economic Studies



Information Technology
Security Master

Military Technical Academy



Advanced Technologies Institute

Conference Partners



Center for Research and Training in
Innovative Techniques of Applied
Mathematics in Engineering



Coding and Storage Theory of
Information Master



SECITC 2021 SCHEDULE

www.secitc.eu

VIDEO CONFERENCE PLATFORM ZOOM FOR THE CONFERENCE DAYS:

<https://ase.zoom.us/j/84978692685?pwd=VIRDbVZJUGtzTXBiUFhyM2RoWUlvdz09>

On line Registration Date:

Starting with 24 November 2021 via [Google Forms RVSP](#)

<https://tinyurl.com/2as4rwve>

DAY 1 - 25 NOVEMBER 2021

Opening Meeting:

Date: 25 November 2021

Hour:

04:30 PM JST (Japan Standard Time)

07:30 AM UTC / GMT (Universal Time Coordinated / Greenwich Mean Time)

08:30 AM CET (Central European Time)

11:30 PM PST (Pacific Standard Time)

Hour-CET	Presenter	Presentation Title	Affiliation
08:30 AM	Welcome Speeches		
	Peter Y. A. RYAN and Cristian TOMA, Conference Chairs		
08:45 AM	Foreword		
	Representatives from:		
	Military Technical Academy	Bucharest University of Economic Studies	
	Department of Computer Science and Military Information Systems	Department of Economic Informatics and Cybernetics	
	Advanced Technologies Institute (ITA)		
09:00 AM	Invited Speakers Session #1		
	Marc JOYE	Functional Circuits: A new paradigm for fully homomorphic encryption	Zama & École Normale Supérieure, FRANCE


SECTION #1
Chair: Cristian TOMA

Hour-CET	Authors	Presentation Title
10:00	Romain Brisse, Simon Boche, Frederic Majorczyk and Jean-Francois Lalande	KRAKEN: A Knowledge-Based Recommender system for Analysts, to Kick Exploration up a Notch
10:30	Somanath Tripathy, Narendra Singh and Divyanshu N Singh	ADAM: Automatic Detection of Android Malware
11:00	Xiaona Zhang	Attack on the Common Prime Version of Murru and Saettone's RSA Cryptosystem
11:30	Md Akhtaruzzaman Adnan, Atika Younus, Md. Harun Al Kawser, Natasha Adhikary, Ahsan Habib and Rakib Ul Haque	Identification of Data Breaches from Public Forums
12:00	Abdul Saboor Malik, Muhammad Khuram Shahzad and Mehdi Hussain	A Forensic Framework for Webmail Threat Detection using Log Analysis

LUNCH / COFFEE BREAK 12:30-13:30
SECTION #2
Chair: Ion BICA

Hour-CET	Authors	Presentation Title
13:30	Johann Groszschaedl	An Evaluation of the Multi-Platform Efficiency of Lightweight Cryptographic Permutations
14:00	Christian Franck and Johann Groszschaedl	Optimized SHA-512 Implementation for 16-bit MSP430 Microcontrollers
14:30	Matteo Rossi, Emanuele Bellini, Anna Hambitzer and Matteo Protopapa	Limitations of the Use of Neural Networks in Black Box Cryptanalysis
15:00	Esra Yeniaras and Murat Cenk	Improved Polynomial Multiplication Algorithms over Characteristic Three Fields and Applications to NTRU Prime
15:30	Evgnosia-Alexandra Kelesidis	An optimization of Bleichenbacher's Oracle Padding Attack
16:00	Daniel Zentai	UC Analysis of the Randomized McElieceCryptosystem



DAY 2 - 26 NOVEMBER 2021

PLENARY SECTION

Hour-CET	Presenter	Presentation Title	Affiliation
Invited Speakers Session #2			
09:00 AM	Mark D. RYAN	Making Privacy Violations Transparent and Accountable	University of Birmingham, UK

SECTION #3

Chair: Cristian CIUREA

Hour-CET	Authors	Presentation Title
10:00	Suthee Ruangwises	Using Five Cards to Encode Each Integer in $Z/6Z$
10:30	Xiaojuan Lu, Bohan Li, Shichang Wang and Dongdai Lin	Conditional Differential Cryptanalysis on Bagua
11:00	Li Duan, Yong Li and Lijun Liao	Perfect Anonymous Authentication and Secure Communication in Internet-of-Things
11:30	Li Duan, Yong Li and Lijun Liao	Flexible Group Non-Interactive Key Exchange in the Standard Model
12:00	Mihai-Zicu Mina and Emil Simion	A Multifunctional Modular Implementation of Grover's Algorithm

LUNCH / COFFEE BREAK 12:30-13:30

SECTION #4

Chair: Marius POPA & Iulian ACIOBANITEI

Hour-CET	Authors	Presentation Title
13:30	George Teseleanu	Lightweight Swarm Authentication
14:00	George Teseleanu and Diana Maimut	New Configurations of Grain Ciphers: Security Against Slide Attacks
14:30	Marian Gusatu and Ruxandra Olimid	Improved security solutions for DDoS mitigation in 5G Multi-access Edge Computing



PLENARY SECTION

Hour-CET	Presenter	Presentation Title	Affiliation
15:00	Invited Speakers Session #3		
	Joshua Guttman	Trust Engineering via Protocol Design: Understanding Attestations from Trusted Execution Environments	MITRE Corporation & Worcester Polytechnic Institute (WPI), USA

SECTION #5

Chair: Diana MAIMUT

Hour-CET	Authors	Presentation Title
16:00	Kashi Neupane	Long-Term Secure Asymmetric Group Key Agreement
16:30	Vlad Craciun and Andrei Mogage	Building De-obfuscated Applications from Polymorphic Binaries
17:00	Cristian Toma, Catalin Boja, Marius Popa, Mihai Doinea and Cristian Ciurea	Viruses, Exploits, Malware and Security Issues on IoT Devices