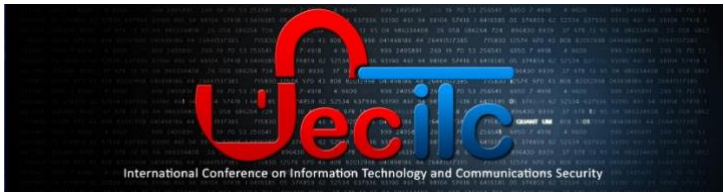
The 18th International Conference on Security for Information Technology and Communications (SecITC2025)

Conference Program



Bucharest, Romania
November 20-21, 2025

Springer

Lecture Notes in Computer Science
LNCS LNAI LNBI

Powered by:

Informatics Security / IT&C Security Master

Bucharest University of Economic Studies

Information Technology Security Master

Military Technical Academy "Ferdinand I"

Advanced Technologies Institute

Conference Chairs

Paolo D'Arco, Università di Salerno, Italy

Alin Zamfiroiu, Bucharest University of Economic Studies, Romania

Keynote Speakers

Maria Isabel Gonzales Vasco

Department of Mathematics, Universidad Carlos III de Madrid, Spain

The Best of Both Worlds: Bridging Classical and Quantum Technologies for Secure Communication

Secure communication in the quantum era requires combining the strengths of classical and quantum technologies. This talk explores hybrid approaches that integrate post-quantum cryptography with quantum key distribution to build resilient and scalable protocols.

Peter Scholl

Department of Computer Science, Aarhus University, Denmark

Zero-Knowledge Proofs and Post-Quantum Signatures From VOLE-in-the-Head

I will introduce a recent paradigm for building zero-knowledge proofs based on vector oblivious linear evaluation (VOLE). VOLE-based proofs are conceptually simple yet powerful, enabling efficient proofs of complex statements with very fast proving times. I will also discuss the use of VOLE-based proofs in the design of post-quantum signature algorithms, including FAEST.

Day 1 - Thursday, November 20, 2025

Time	Presentation	Hall name
09:00 - 09:30	**Registration** **&** **Coffee break**	**Aula Magna Entry Hall**
09:30 - 09:45	**Welcome Speeches** Paolo D'Arco and Alin Zamfiroiu Conference chairs	**Aula Magna**
09:45 - 10:00	**Foreword** Representatives from: Military Technical Academy "Ferdinand I" Bucharest University of Economic Studies Advanced Technologies Institute (ITA)	
10:00 - 10:45	**Keynote speaker** **Maria Isabel Gonzales Vasco**, Department of Mathematics, Universidad Carlos III de Madrid *"The Best of Both Worlds: Bridging Classical and Quantum Technologies for Secure Communication"*	**Aula Magna**
10:45 – 11:00	**Q&A**	

BREAK 11.00-11.20

SESSION #1

Session chair: Ion Bica, Cătălin Boja

Hall name: Robert Schumann Room

TIME	AUTHORS	PRESENTATION TITLE
11:20	Matteo Steinbach, Johann Groszschaedl And Peter Roenne	Hard-To-Find Bugs In A Post-Quantum Age
11:40	Michail Takaronis, Vasileios Gkioulos, Georgios Kavallieratos and Jia-Chun Lin	Applying SOA Principles to Next-Generation Cyber Range Design
12:00	Watung Budiman, Ford Gaol, Haryono Soeparno and Yulyani Arifin	Hierarchical Hashing for End-to-End Integrity in HTTP Live Streaming (HLS)
12:20	Sara Nikula	Combining digital signatures and key recycling in QKD authentication: a performance and security analysis

BREAK 12.40-14.00

SESSION #2

Session chair: Diana Maimut

Hall name: Robert Schumann Room

TIME	AUTHORS	PRESENTATION TITLE
14:00	Taisei Mstsushita, Sohto Chiku, Keisuke Hara and Junji Shikata	Adaptively Secure Matchmaking Encryption from Witness Encryption
14:20	Shun Odaka and Yuichi Komano	Card-based Representation of Floating-point Numbers and Arithmetic Operations
14:40	Hayato Gibo, Yohei Watanabe and Mitsugu Iwamoto	Adding Two Easy Functions Is Always Hard to Invert
15:00	Towa Toyooka, Yohei Watanabe and Mitsugu Iwamoto	Efficiency Improvement of Deniable FHE: Tighter Deniability Analysis and TFHE-based Construction

BREAK 15.20-15.40

SESSION #3

Session chair: Noaman Ali Syed

Hall name: Robert Schumann Room

TIME	AUTHORS	PRESENTATION TITLE
15:40	Rownak Borhan, Yuzo Taenaka and Youki Kadobayashi	DILISAES: An Experimental Lattice-Based Post-Quantum Signcryption Scheme
16:00	Lucía Muñoz Solanas and Álvaro Fernández Carrasco	Q-PROTECT: Towards Quantum-Safe Cryptography in 5G Networks
16:20	Shudarsan Regmi and Saravanan Selvam	Securing LLM-Integrated Chatbots: A Transformer-Based Vulnerability Scanner for Prompt Injection and Jailbreak Detection
16:40	Alin Zamfiroiu, George Orzanescu, Joe Francom and Noaman Ali Syed	Machine Learning-Based Web Application Firewalls for SQL Injection and XSS Prevention

Day 2 - Friday, November 21, 2025

Time	Presentation	Hall name
09:00-09:30	**Registration & Coffee break**	**Aula Magna Entry Hall**
09:30 – 10:15	**Keynote speaker** **Peter Scholl,** Department of Computer Science, Aarhus University "*Zero-Knowledge Proofs and Post-Quantum Signatures From VOLE-in-the-Head*"	**Aula Magna**
10:15 – 10:25	**Q&A**	
10:25 – 10:40	**Scientific Research Results & Dissemination** Strengthening Synergies in Defence and Civilian Cybersecurity (ECYBRIDGE), https://ecybridge.eu/ Ion Bica, Diana Maimuț, Stefania Nițâ	**Aula Magna**

BREAK 10.40-11.00

SESSION #4

Session chair: Iulian Aciobăniței

Hall name: Robert Schumann Room

TIME	AUTHORS	PRESENTATION TITLE
11:00	Ren Igari, Yuichi Komano and Takaaki Mizuki	Suken BINGO: An Application of Card-based Cryptography to Psychological Board Games
11:20	Kashi Neupane	Deniable Asymmetric One-Round Group Key Agreement
11:40	Ștefania Ștefănescu and Mirabela Medvei	Enhancing Keycloak with Verifiable Audit Trails for Identity and Access Management - A Merkle Tree Approach
12:00	Aliyu Tanko Ali, Damas Gruska and Martin Leucker	Supervised Attack Trees

BREAK 12.20-12.40

SESSION #5

Session chair: Cristian Toma

Hall name: Robert Schumann Room

TIME	AUTHORS	PRESENTATION TITLE
12:40	Orçun Çetin and Nazlı Bıyıklı	This Time, Make It Intentional: Evaluating the Efficacy of Large Language Models for Automated Vulnerable Code Generation
13:00	Shoya Nakamura, Kunio Akashi and Yuji Sekiya	Proposal and evaluation of a method for Container Micro-Segmentation
13:20	Catalin Cot, Adrian Viorel Colesa and Radu Marian Portase	Rust in the Kernel: A Practical Evaluation on Windows
13:40	Teodor Cervinski, Cristian Toma, Catalin Boja, Marius Popa, Claudiu Brandas and Andrei Cazacu	Hybrid Deep Learning and QNN for detecting attacks within IoT Networks