The Eighth Symposium on Cyber Security, Cryptology and Machine Learning (CSCML 2024)

December 19-20, 2024

Tentative Full Program Schedule

Thursday, December 19, 2024				
Time	Main Room/ Academic Research Track		Other Tracks	
8:00- 8:10 Israel Time GMT +2	**Opening Speech:** **Professor Shlomi Dolev**			
8:15- 08:55 Israel Time GMT+2	**Keynote Speaker 1: Andrew C. Yao** Dean of the Institute for Interdisciplinary Information Sciences (IIIS) at Tsinghua University **Talk Titled:** *Cryptography in the Age of Bio, Quantum and AI* Hosted By: Giuseppe Persiano		8:15- 8:45	Zoom Meeting to open the competition. CAPTURE THE FLAG
9:00- 10:35 Israel Time GMT +2	**Academic Track: Morning Session** Moderator: Michael Eldad		**PhD/ Masters Track Session 1:** Moderator: Oded Margalit	
	9:00- 9:20	**Polynomial Adaptation of Large-Scale CNNs for Homomorphic Encryption-Based Secure Inference** Moran Baruch, Nir Drucker, Gilad Ezov, Eyal Kushnir, Jenny Lerner, Yoav Goldberg, Omri Soceanu and Itamar	9:05- 9:10	Welcome and Instructions
	9:20- 9:40	**Password-authenticated Cryptography from Consumable Tokens** Ghada Almashaqbeh	9:10- 9:20	
	9:40- 10:00	**Robust Secure Aggregation for Co-located IoT Devices with Corruption Localization** Giovanni Di Crescenzo, Elina van Kempen and Gene Tsudik	9:20- 9:30	
			9:30- 9:40	
	10:00 10:20	**Spoofing-robust speaker verification based on time-domain embedding** Avishai Weizman, Yehuda Ben-Shimol and Itshak Lapi	9:40-	

	10:20- 10:40	**A Probabilistic Model for Rounding Errors: A New Look at the Table-Maker’s Dilemma** Jonathan Devor, Daniel Khankin, and Oded Margalit	9:50	
	Short: 10:40- 10:50	**Behavior-Driven Access Policy Prediction** Shmuel Amour and Ehud Gudes	9:50- 10:00	
10:50- 12:50 Israel Time GMT +2	**Academic Track: Mid-Morning Session** Moderator:		**PhD/ Masters Track Session 2:** Moderator:	
	10:50- 11:10	**Provable Imbalanced Point Clustering** David Denisov, Dan Felmdan, Shlomi Dolev and Michael Segal	10:45- 10:50	Welcome and Instructions
	11:30- 11:50	**Mezzo TLS 1.3 protocol, suitable for transmitting already-encrypted data** Nir Drucker and Shay Gueron	10:50- 11:00	
	11:50- 12:10	**LLMSecCode: Evaluating Large Language Models for Secure Coding** Anton Rydén, Erik Näslund, Elad Michael Schiller and Magnus Almgren	11:00- 11:10	
	12:10- 12:30	**Distributed Verifiable Random Function with Compact Proof** Ahmet Ramazan Ağırtaş, Arda Buğra Özer, Zülfükar Saygı and Oğuz Yayla	11:10- 11:20	
	Short: 12:30- 12:40	**On the overflow and p-adic theory applied to homomorphic encryption** Jacob Blindenbach, Jung Hee Cheon, Gamze Gursoy and Jiayi Kang	11:20- 11:30	
	Short: 12:40- 12:50	**Beneath the Cream: Unveiling Relevant Information Points from CrimeBB with Its Ground Truth Labels** Felipe Moreno, Daniel Sadoc Menasche and Cabral Lima	11:30- 11:40	
			11:40- 11:50	
			11:50- 12:00	

13:00-13:45 Israel Time GMT +2		**Keynote Speaker 2: Esti Peshin** VP & General Manager of the Cyber Division at the Israel Aerospace Industries Ltd. **Talk Titled: TBA** Hosted by: Michael Elhadad		
13:50-14:40 Israel Time GMT +2		**Academic Track: Noon Session** Moderator:		**Entrepreneurship Session 2:** Moderator:
	13:50-14:10	**Fiat-Shamir in the Wild** Duy Hieu Nguyen, Huynh Thanh Uyen Ho and Alex Biryukov	12:20-12:30	Welcome and Instructions
	12:40-13:00	**Predicting the degradation rate of technical systems at early stages of development** Sergey Frenkel	12:30-12:40	
	13:00-13:20	**Brief Announcement: Reminisce for Securing Private-keys in Public** Shlomi Dolev, Komal Kumari, Sharad Mehrotra, Baruch Schieber and Shantanu Sharma	12:40-12:50	
	13:20-13:40	**Minimally Intrusive Access Management to CDNs based on Models and Access Patterns** Lenise Rodrigues, Daniel Menasché, Arthur Serra and Antônio Rocha	13:00-13:00	
	Short: 13:40-14:00	**Cybersecurity Enhancement for Wireless Networks Using Aerial Reconfigurable Intelligent Surfaces** Rajnish Kumar and Shlomi Arnon	13:00-13:10	
	Short: 14:00-14:10	**KNN+X** Daniel Gilkarov, Lee-Ad Gottlieb and Hillel Oyahon	13:10-13:40	**Voting for the Three Best Pitches and wrapping up the session.** The three best pitches will present their pitches again for 5 minutes each in front of the whole audience (main room) from 16:50-17:20, for a finalist to be chosen.
	Short: 14:10-14:20	**(Short Paper) Challenges in Timed-Cryptography: A Position Paper** Karim Eldefrawy, Benjamin Terner and Moti Yung		

14:20 14:40 Israel Time GMT +2		**Pitch Finalist Ceremony** *Hosted By:* **The three finalists from the Entrepreneurship (Pitch) Track will have 5 minutes to present their pitch again before the entire audience of CSCML. Then the audience will get to vote for the best pitch.**	
14:40- 15:25 Israel Time GMT +2		**Keynote Speaker 3: Roberto Baldoni** Former Director General at National Cybersecurity Agency of Italy **Talk Titled: TBA** Hosted by: Mirosław Kutyłowski	
15:30- 17:40 Israel Time GMT +2		**Academic Track: Evening Session** Moderator:	
	15:30- 15:50	**On the Effects of Neural Network-based Output Prediction Attacks on the Design of Symmetric-key Ciphers** Hayato Watanabe, Ryoma Ito and Toshihiro Ohigashi	
	15:50- 16:10	**Entanglement-based Mutual Quantum Distance Bounding** Aysajan Abidin, Karim Eldefrawy and Dave Singelee	
	16:10- 16:30	**Evaluation of Posits for Spectral Analysis Using a Software-Defined Dataflow Architecture** Sameer Deshmukh, Daniel Khankin, William Killian, John Gustafson and Elad Raz	
	Short: 16:30- 16:40	**OWF Candidates Based on: Xors, Error Detection Codes, Permutations, Polynomials, Interaction, and Nesting** Paweł Cyprys, Shlomi Dolev and Oded Margali	
	Short: 16:40- 16:50	**Super-Teaching in Machine Learning** Dina Barak-Pelleg, Daniel Berend and Aryeh Kontorovich	
	Short: 16:50- 17:00	**A Lattice Attack Against a Family of RSA-like Cryptosystems** George Teseleanu	
	Short: 17:10- 17:20	**On the security-related properties of randomly constructed combinatorial structures** Vasiliki Liagkou, Panagiotis Nastou, Paul Spirakis and Yannis Stamatiou	

	Short: 17:20-17:30	**HBSS+: Simple Hash-Based Stateless Signatures revisited** Przemysław Kubiak and Oliwer Sobolewski	
17:35 18:00 Israel Time GMT+2		**Closing Ceremony/ Blessing** **Hosted by: Professor Shlomi Dolev**	

Friday, December 20 2024	
Time	**Event**
11:00-11:15 Israel Time GMT+2	**Welcome** Hosted by: Professor Shlomi Dolev

11:20-12:00 **Israel Time** **GMT+2**	**Keynote Speaker 3: Elad Raz** **Founder of NextSilicon** **Talk Titled: Reimagining Innovation: Overcoming Challenges to Lead the Next Generation of Compute** Hosted by: Oded Margalit
12:05-12:45 **Israel Time** **GMT+2**	**Keynote Speaker 4: Claire Vishik** **Senior Director of Trust Technology & Policy and a Senior Principal Engineer at Intel.** **Talk Titled: TBA** Hosted by:
12:45-13:25 **Israel Time** **GMT+2**	**Keynote Speaker 5:** Sol (Shlomo) Gradman **CEO ASG Ltd., Chairman, Israel High Tech CEO Forum, [Founder of ChipEx, iNNOVEX, DevelopEX & Silicon Club]** **Talk Titled: TBA** Hosted by: Shlomi Dolev
13:25-14:05 **Israel Time** **GMT+2**	**ZOOM LECTURE – ISRAEL IN BIBLICAL TIMES**
14:05-14:30 **Israel Time** **GMT+2**	**Closing Ceremony/ Blessing** **Hosted by: Professor Shlomi Dolev**