

# CSCML 2018

## Second International Symposium on Cyber Security, Cryptography and Machine Learning

June 21-22, 2018, Beer-Sheva, Israel

<http://www.cs.bgu.ac.il/~fradmin/cscml18>

### General Chairs and Conference Committee

Shlomi Dolev, Co-Chair *Ben-Gurion Univ., Israel*  
Sachin Lodha, Co-Chair *Tata CS, India*  
Timi Budai, Organizing Chair *Ben-Gurion Univ., Israel*

### Academic Research Track Program Committee

Yehuda Afek *Tel-Aviv Univ., Israel*  
Adi Akavia *Tel-Aviv Yaffo Academic College, Israel*  
Amir Averbuch *Tel-Aviv Univ., Israel*  
Roberto Baldoni *Univ. di Roma "La Sapienza", Italy*  
Michael Ben-Or *Hebrew Univ., Israel*  
Anat Bremner-Barr *IDC Herzliya, Israel*  
Ran Canetti *Boston Univ., USA & Tel-Aviv Univ., Israel*  
Itai Dinur, PC Co-Chair *Ben-Gurion Univ., Israel*  
Karim ElDefrawy *SRI International, USA*  
Bezalel Gavish *Southern Methodist University, USA*  
Yossi Gilad *Boston Univ. and MIT, USA*  
Niv Gilboa *Ben-Gurion Univ., Israel*  
Shafi Goldwasser *Weizmann Institute and MIT, USA*  
Ehud Gudes *Ben-Gurion Univ., Israel*  
Shay Gueron *Univ. of Haifa, Israel*  
Carmit Hazay *Bar Ilan Univ., Israel*  
Danny Hendler *Ben-Gurion Univ., Israel*  
Amir Herzberg *UCONN and Bar-Ilan Univ., Israel*  
Stratis Ioannidis *Northeastern Univ., USA*  
Gene Itkis *MIT Lincoln Laboratory, USA*  
Nathan Keller *Bar Ilan Univ., Israel*  
Sarit Kraus *Bar Ilan Univ., Israel*  
Mark Last *Ben-Gurion Univ., Israel*  
Guy Leshem *Ashkelon Academic College, Israel*  
Ximing Li *South China Agricultural Univ., China*  
Yin Li *Fudan Univ., China*  
Michael Luby *Qualcomm, USA*  
Avi Mendelson *Technion, Israel*  
Aikaterini Mitrokotsa *Chalmers Univ. Tech., Sweden*  
Benny Pinkas *Bar Ilan Univ., Israel*  
Ely Porat *Bar-Ilan Univ., Israel*  
Dan Raz *Technion, Israel*  
Christian Riess *FAU, Germany*  
Elad M. Schiller *Chalmers Univ. Tech., Sweden*  
Galina Schwartz *UC Berkeley, USA*  
Gil Segev *Hebrew Univ., Israel*  
Haya Shulman *Fraunhofer SIT, Germany*  
Paul Spirakis *U. of Liverpool, UK & U. Patras, Greece*  
Naftali Tishby *Hebrew Univ., Israel*  
Ari Trachtenberg *Boston Univ., USA*  
Philippos Tsigas *Chalmers Univ. Tech., Sweden*  
Doug Tygar *UC Berkeley, USA*  
Kalyan Veeramachaneni *MIT, USA*  
Michael Waidner *Fraunhofer SIT & TU Darmstadt, DE*  
Rebecca Wright *Rutgers Univ., USA*  
Moti Yung *Columbia Univ. and Snapchat, USA*

### Entrepreneurship Track Program Committee

Ran Achituv *Entrée Capital, Israel*  
Sitaram Chamarty, PC Co-Chair *Tata CS, India*  
Dorit Dor *Check Point, Israel*  
Gili Elkin *Israel-Colorado Innovation Fund, Israel*  
Sol Fayerman-Hansen *Bank of Montreal, Israel*  
Ben Gilad *Tata CS, Israel*  
Roman Gold *JSCapital, Israel*  
Shlomo Gradman *ASG, Ltd., Israel*  
Yona Hollander *Fortscale, Israel*  
Guy Horowitz *Deutsche Telekom Capital Partners, Israel*  
Ayal Itzkovitz *Pitango Venture Capital, Israel*  
Arik Kleinstein *Glilot Capital Partners, Israel*  
Adi Levanon *Symmetrical Ventures, Israel*  
Oded Margalit *IBM, Israel*  
Yossi Moldawsky *PlusVentures, Israel*  
Nir Netzer *Equitech, Israel*  
Hagai Ortner *Magna BSP, Israel*  
Michael Rodeh *Permira and Land & Expand, Israel*  
Yaron Rosenbaum *Iris Capital, Israel*  
Yuval Shachar *Innovation Endeavors, Israel*  
Yaakov Stein *RAD Data Communications, Israel*  
Dan Tseitou *Bonotec, Israel*  
Yoav Tzruya *JVP Cyber Labs, Israel*  
Yael Villa *CISCO, Israel*  
Yaron Wolfsthal *IBM, Israel*  
Uzy Zwebner *ATP and BaseCamp, Israel*

### Dates

Submission deadline ~~March 18, 2017~~ **Extended to March 28, 2018 for title & abstract**  
Acceptance notification **April 15, 2018**  
Camera-ready copy due **April 20, 2018**

### Steering Committee

Orna Berry *DELLEMC, Israel*  
Shlomi Dolev, Chair *Ben-Gurion Univ., Israel*  
Yuval Elovici *Ben-Gurion Univ., Israel*  
Ehud Gudes *Ben-Gurion Univ., Israel*  
Jonathan Katz *Univ. of Maryland, USA*  
Rafail Ostrovsky *UCLA, USA*  
Jeffrey D. Ullman *Stanford Univ., USA*  
Kalyan Veeramachaneni *MIT, USA*  
Yaron Wolfsthal *IBM, Israel*  
Moti Yung *Columbia Univ. and Snapchat, USA*

**Scope.** Original contributions to the theory, design, analysis, implementation, or application of cyber security, cryptography and machine learning systems and networks, and, in particular, of conceptually innovative results are solicited. Topics of interest include, but are not limited to:

- **Cyber Security Design** Secure Software Development methodologies, Formal methods, Semantics and verification of secure systems, Fault tolerance, Reliability, Availability of distributed secure systems, Game-theoretic approaches to secure computing, Automatic recovery, Self-stabilizing, and self-organizing systems, Communication, Authentication and identification, Cyber security for mobile and Internet of Things, Cyber security of corporations, Security and privacy for cloud, Edge and fog computing, Cryptocurrency, and Blockchain
- **Cryptography** Cryptographic implementation analysis and construction, Secure multi-party computation, Privacy-enhancing technologies and anonymity, Post-quantum cryptography and security
- **Machine Learning and Big Data** Anomaly detection and malware identification, Business Intelligence and Security, Digital forensics, Digital rights management, Trust management and reputation systems, Information retrieval, Risk analysis, DoS

Conference presentations will have two formats (you can find more information about the formats from last year's event by clicking on the following link: <https://www.cs.bgu.ac.il/~fradmin/cscml17/submission.html>):

**1. Regular presentations** of 25 minutes accompanied by papers of up to 15 pages in the proceedings. This form is intended for contributions reporting on original research, submitted exclusively to this conference.

**2. Entrepreneurship pitch** of 5 to 10 minutes accompanied by six page abstracts/pitch presentation. (See also: <https://www.cs.bgu.ac.il/~frankel/TechnicalReports/2017/17-03.pdf>)

**Submission.** Papers are to be submitted electronically, following the guidelines available on the conference web page.

Each submission must be in English, in PDF format, and begin with a cover page including: (1) the title, (2) the names and affiliations of all authors, (3) contact author's email, address and telephone number, (4) a brief, one paragraph abstract of the paper, (5) indication whether the paper is a regular submission, or an entrepreneurship pitch submission (the authors of the entrepreneurship pitch track please note that the submissions will not be NDA protected).

A regular submission must not exceed 15 (LNCS formatted) single-column pages (excluding cover page and references). Additional necessary details may be included in a clearly marked appendix that will be read at the discretion of the program committee. An entrepreneurship pitch submission must not exceed 6 single-column pages. All submissions must use LNCS format, and any submission deviating from these guidelines will be rejected without consideration of its merit.

It is recommended that a regular submission begin with a succinct statement of the problem or the issue being addressed, a summary of the main results or conclusions, a brief explanation of their significance, a brief statement of the key ideas, and a comparison with related work, all tailored to a non-specialist. Technical development of the work, directed to the specialist, should follow. Papers outside of the conference scope will be rejected without review.

If requested by the authors on the cover page, a regular submission may also be considered for the entrepreneurship pitch track.

**Publication.** Regular papers will be included in the Springer LNCS conference proceedings. Extended and revised versions of selected papers will be considered for a special issue of the journal *Information and Computation*.

**Additional Planned Events.** PhD Track and "Capture the Flag" Hackathon are planned to take place at CSCML 2018.