



Crypto 2018 – Affiliated Events!!

2018 AUGUST

SUN	MON	TUE	WED	THU	FRI	SAT
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
Crypto	Crypto	Crypto	Crypto	Crypto		
26	27	28	29	30	31	

2018 AUGUST

SUN	MON	TUE	WED	THU	FRI	SAT
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17 Workshop	18 Workshop
19 Workshop Crypto	20 Crypto	21 Crypto	22 Crypto	23 Crypto	24	25
26	27	28	29	30	31	

Decentralized Cryptocurrencies and Blockchains - 1

Friday, August 17, 2018

Organizers: Ittai Abraham, Eli Ben-Sasson, Alessandro Chiesa, Dahlia Malkhi

- David Mazières (Stanford / Stellar)
- Vitalik Buterin (Ethereum)
- Zooko Wilcox (Zcash)
- Peter Van Valkenburgh (Coin Center)
- Joshua Slayton (Coinlist)
- Mic Bowman (Intel)

Decentralized Cryptocurrencies and Blockchains - 2

Saturday, August 18, 2018

Organizers: Ittai Abraham, Eli Ben-Sasson, Alessandro Chiesa, Dahlia Malkhi

- Thaddeus Dryja (MIT, Lightning Network)
- Dawn Song (UC Berkeley)
- Silvio Micali (MIT)
- Rafael Pass (Cornell Tech / Thunderella)
- Panel

Quantum Safe Crypto for Industry

Saturday, August 18, 2018

Organizers: Matt Campagna, Jean-Charles Faugère, Ludovic Perret, Rafael Misoczki

- Lily Chen (NIST)
- Aline Gouget (Gemalto)
- Shay Gueron (University of Haifa and Amazon)
- Brian LaMacchia (Microsoft)
- Adam Langley (Google)
- Rafael Misoczki (Intel)
- Michele Mosca (U. Of Waterloo, IQC and EvolutionQ)

Workshop on Attacks in Cryptography (WAC)

Saturday, August 18, 2018

Organizers: Nadia Heninger

- Matt Green (Johns Hopkins)
- Kenny Patterson (Royal Holloway)
- Juraj Somorovsky (RU Bochum)
- Hovav Shacham (University of Texas, Austin)
- Christina Garman (Purdue)
- Mathy Vanhoef (KU Leuven)
- Petr Svenda and Marek Sys (Masaryk University)
- Daniel J. Bernstein and Tanja Lange ([why I got the full 3 minutes](#))

Beyond Crypto: A TCS Perspective

Sunday, August 19, 2018

Organizers: Yuval Ishai, Guy Rothblum

- Scott Aaronson (UT Austin)
- Boaz Barak (Harvard)
- Cynthia Dwork (Harvard)
- Aleksander Madry (MIT)
- Virginia Vassilevska Williams (MIT)
- Mary Wootters (Stanford)

Crypto Welcomes TLS 1.3 (CWTLIS 1.3)

Sunday, August 19, 2018

Organizers: Hugo Krawczyk, Kenny Paterson

- Karthikeyan Bhargavan (INRIA)
- Cas Cremers (Oxford University)
- Marc Fischlin (Technische Universität Darmstadt)
- Kenny Paterson (Royal Holloway, University of London)
- Eric Rescorla (Mozilla)

Encryption and Surveillance

Sunday, August 19, 2018

Organizers: Timothy Edgar, Joan Feigenbaum, Daniel J. Weitzner

- Senior government officials from around the globe
- Human-rights advocates
- Technical experts

MathCrypt

Sunday, August 19, 2018

Organizers: Jintai Ding, Jung Hee Cheon, Kristin Lauter

- Paper submission deadline June 1, 2018

Pay-per-Day

- Attend any workshop on the same day
- Heavy discounts if also attending crypto



Home

Twitter – Use #crypto2018

Technical Program

Call for Papers

Paper Submission

Accepted Papers

Program

Rump Session

Affiliated Events

List of Affiliated Events

- Cryptocurrencies
- Quantum (QsCI)
- Attacks (WAC)
- Beyond Crypto (TCS)
- TLS 1.3
- Enc. and Surveillance
- MathCrypt

Call for Affiliated Events

General Information

Code of Conduct

Registration



Crypto 2018

August 19-23, 2018

Affiliated events

August 17-19, 2018

Santa Barbara, USA

Register: pay per day of affiliated events on the Crypto 2018 registration page. [Follow @IACRcrypto](#)

Affiliated Events Organizers: Elette Boyle (chair), Fabrice Benhamouda, Tal Rabin

Friday, August 17, 2018

Decentralized Cryptocurrencies and Blockchains (Part I)

Organizers: Ittai Abraham (VMware), Eli Ben-Sasson (Technion), Alessandro Chiesa (UC Berkeley), Dahlia Malkhi (VMware)

Saturday, August 18, 2018

Decentralized Cryptocurrencies and Blockchains (Part II)

Organizers: Ittai Abraham (VMware), Eli Ben-Sasson (Technion), Alessandro Chiesa (UC Berkeley), Dahlia Malkhi (VMware)

Quantum-safe Cryptography for Industry (QsCI)

Organizers: Matt Campagna (Amazon), Jean-Charles Faugère (INRIA, Sorbonne Université, CNRS), Ludovic Perret (Sorbonne Université, INRIA, CNRS), Rafael Misoczki (Intel)

Workshop on Attacks in Cryptography (WAC)

Organizers: Nadia Heninger (University of Pennsylvania)

Sunday, August 19, 2018

Beyond Crypto: A TCS Perspective

Organizers: Yuval Ishai (Technion), Guy Rothblum (Weizmann)

Crypto Welcomes TLS 1.3 (CWTLs 1.3)

Organizers: Hugo Krawczyk (IBM Research), Kenny Paterson (Royal Holloway)

Encryption and Surveillance

Organizers: Timothy Edgar (Watson Institute, Brown University), Joan Feigenbaum (Computer Science Department, Yale University), Daniel J. Weitzner (Internet Policy Research Institute, MIT)

MathCrypt 2018

Organizers: Jintai Ding (University of Cincinnati), Jung Hee Cheon (Seoul National University), Kristin Lauter (Microsoft Research)

Click on the title to see the abstract, and on the button to access the website of the event.