

Special thanks to our sponsors



Hiroshi Fujiwara
Cyber Security
Research Center

Diamond Sponsor:

arm

Gold Sponsors:



Silver Sponsors:



AUDITCHAIN



CHECK POINT
INSTITUTE FOR
INFORMATION SECURITY

IBM Research



RAFAEL
ADVANCED DEFENSE SYSTEMS LTD.

Sponsors:



INPUT | OUTPUT



Prime Minister's Office
National Cyber Directorate

Rambus



TECHNION
Israel Institute of Technology



אוניברסיטת חיפה
University of Haifa
جامعة حيفا



EUROCRYPT2018

APRIL 29 - MAY 3, 2018 | TEL-AVIV, ISRAEL

Conference Program

Main hall (Israel A)	
08:00-09:00	Registration, coffee & light breakfast
09:00-09:10	Opening Remarks General Chair, Orr Dunkelman
09:10-09:15	Track-switch break
09:15-10:55	Foundations Chair: Alon Rosen
	On the Bit Security of Cryptographic Primitives Daniele Micciancio, Michael Walter
	On the Gold Standard for Security of Universal Steganography Sebastian Berndt, Maciej Liśkiewicz
	Memory Lower Bounds of Reductions Revisited Yuyu Wang, Takahiro Matsuda, Goichiro Hanaoka, Keisuke Tanaka
	Fiat-Shamir and Correlation Intractability from Strong KDM-Secure Encryption Ran Canetti, Yilei Chen, Leonid Reyzin, Ron D. Rothblum
10:55-11:25	Coffee break
11:25-12:40	Random Oracle Model Chair: Yevgeniy Dodis
	Random Oracles and Non-Uniformity Sandro Coretti, Yevgeniy Dodis, Siyao Guo, John P. Steinberger
	Another Step Towards Realizing Random Oracles: Non-Malleable Point Obfuscation Ilan Komargodski, Eylon Yogev
	The Wonderful World of Global Random Oracles Jan Camenisch, Manu Drijvers, Tommaso Gagliardoni, Anja Lehmann, Gregory Neven

Side hall (Israel C+D)	
08:00-09:00	Registration, coffee & light breakfast
09:00-09:10	Opening Remarks Main hall (Israel A) only
09:10-09:15	Track-switch break
09:15-10:55	Lattices Chair: Muthuramakrishnan Venkatasubramanian
	Shortest Vector from Lattice Sieving: a Few Dimensions for Free Léoucas
	On the Ring-LWE and Polynomial-LWE problems Miruna Rosca, Damien Stehlé, Alexandre Wallet
	Faster Gaussian Sampling for Trapdoor Lattices with Arbitrary Modulus Nicholas Genise, Daniele Micciancio
	Short, Invertible Elements in Partially Splitting Cyclotomic Rings and Applications to Lattice-Based Zero-Knowledge Proofs Vadim Lyubashevsky, Gregor Seiler
10:55-11:25	Coffee break
11:25-12:40	Fully Homomorphic Encryption Chair: Vinod Vaikuntanathan
	Homomorphic Lower Digits Removal and Improved FHE Bootstrapping Hao Chen, Kyoohyung Han
	Homomorphic SIM²D Operations: Single Instruction Much More Data Wouter Castryck, Ilia Iliashenko, Frederik Vercauteren
	Bootstrapping for Approximate Homomorphic Encryption Jung Hee Cheon, Kyoohyung Han, Andrey Kim, Miran Kim, Yongsoo Song

	Main hall (Israel A)
12:40-14:10	Lunch
14:10-15:10	Invited Talk Chair: Vincent Rijmen
	Desperately Seeking Sboxes Anne Canteaut
15:10-15:40	Coffee break
15:40-16:30	Permutations Chair: Bart Preneel
	Full Indifferentiable Security of the Xor of Two or More Random Permutations Using the X^2 Method Srimanta Bhattacharya, Mridul Nandi
	An Improved Affine Equivalence Algorithm for Random Permutations Itai Dinur
16:30-16:35	Track-switch break
16:35-17:25	Galois Counter Mode Chair: Tomer Ashur
	Optimal Forgeries Against Polynomial-Based MACs and GCM Atul Luykx, Bart Preneel
	Revisiting AES-GCM-SIV: Multi-user Security, Faster Key Derivation, and Better Bounds Priyanka Bose, Viet Tung Hoang, Stefano Tessaro

	Side hall (Israel C+D)
12:40-14:10	Lunch
14:10-15:10	Invited Talk Main hall (Israel A) only
15:10-15:40	Coffee break
15:40-16:30	Attribute-Based Encryption Chair: Carmit Hazay
	Unbounded ABE via Bilinear Entropy Expansion, Revisited Jie Chen, Junqing Gong, Lucas Kowalczyk, Hoeteck Wee
	Anonymous IBE, Leakage Resilience and Circular Security from New Assumptions Zvika Brakerski, Alex Lombardi, Gil Segev, Vinod Vaikuntanathan
16:30-16:35	Track-switch break
16:35-17:25	Secret Sharing Chair: Yuval Ishai
	Towards Breaking the Exponential Barrier for General Secret Sharing Tianren Liu, Vinod Vaikuntanathan, Hoeteck Wee
	Improving the Linear Programming Technique in the Search for Lower Bounds in Secret Sharing Oriol Farràs, Tarik Kaced, Sebastià Martín, Carles Padró

	Main hall (Israel A)	
08:00-09:00	Coffee & light breakfast	
09:00-09:50	Blockchain	Chair: Ivan Visconti
	Thunderella: Blockchains with Optimistic Instant Confirmation Rafael Pass, Elaine Shi	
	But Why Does it Work? A Rational Protocol Design Treatment of Bitcoin Christian Badertscher, Juan A. Garay, Ueli Maurer, Daniel Tschudi, Vassilis Zikas	
09:50-09:55	Track-switch break	
09:55-10:45	Blockchain (Cont.)	Chair: Ivan Visconti
	Ouroboros Praos: An adaptively-secure, semi-synchronous proof-of-stake blockchain Bernardo David, Peter Gazi, Aggelos Kiayias, Alexander Russell	
	Sustained Space Complexity Joël Alwen, Jeremiah Blocki, Krzysztof Pietrzak	
10:45-11:15	Coffee break	
11:15-12:30	Private Simultaneous Messages	Chair: Yuval Ishai
	The Communication Complexity of Private Simultaneous Messages, Revisited Benny Applebaum, Thomas Holenstein, Manoj Mishra, Ofer Shayevitz	
	The Complexity of Multiparty PSM Protocols and Related Models Amos Beimel, Eyal Kushilevitz, Pnina Nissim	

	Side hall (Israel C+D)	
08:00-09:00	Coffee & light breakfast	
09:00-09:50	Multi-Collision Resistance	Chair: Jens Groth
	Multi-Collision Resistant Hash Functions and their Applications Itay Berman, Akshay Degwekar, Ron D. Rothblum, Prashant Nalini Vasudevan	
	Collision Resistant Hashing for Paranoids: Dealing with Multiple Collisions Ilán Komargodski, Moni Naor, Eylon Yogev	
09:50-09:55	Track-switch break	
09:55-10:45	Signatures	Chair: Jens Groth
	Synchronized Aggregate Signatures from the RSA Assumption Susan Hohenberger, Brent Waters	
	More Efficient (Almost) Tightly Secure Structure-Preserving Signatures Romain Gay, Dennis Hofheinz, Lisa Kohl, Jiaxin Pan	
10:45-11:15	Coffee break	
11:15-12:30	Masking	Chair: Gaëtan Leurent
	Formal Verification of Masked Hardware Implementations in the Presence of Glitches Roderick Bloem, Hannes Gross, Rinat Iusupov, Bettina Könighofer, Stefan Mangard, Johannes Winter	
	Masking the GLP Lattice-Based Signature Scheme at Any Order Gilles Barthe, Sonia Belaid, Thomas Espitau, Pierre-Alain Fouque, Benjamin Grégoire, Mélissa Rossi, Mehdi Tibouchi	
	Masking Proofs are Tight, and How to Exploit it in Security Evaluations Vincent Grosso, François-Xavier Standaert	

	Main hall (Israel A)
12:30-14:00	Lunch
14:00-14:25	Best Young Research Award Chair: Eike Kiltz
	The Discrete-Logarithm Problem with Preprocessing Henry Corrigan-Gibbs, Dmitry Kogan
14:25-15:40	Best Paper Awards Chair: Eike Kiltz
	Simple Proofs of Sequential Work Bram Cohen, Krzysztof Pietrzak
	Two-Round Multiparty Secure Computation from Minimal Assumptions Sanjam Garg, Akshayaram Srinivasan
	k-Round Multiparty Computation from k-Round Oblivious Transfer via Garbled Interactive Circuits Fabrice Benhamouda, Huijia Lin

	Rump Session - Main hall (Israel A)
18:30-19:30	Rump Session Reception
19:30-21:00	Rump Session Chairs: Daniel J. Bernstein and Tanja Lange
21:00-21:30	Break
21:30-23:00	Rump Session (Cont.)

	Side hall (Israel C+D)
12:30-14:00	Lunch
14:00-14:25	Best Young Research Award Main hall (Israel A) only
14:25-15:40	Best Paper Awards Main hall (Israel A) only

18:30-23:00	Rump Session Main hall (Israel A) only

	Main hall (Israel A)
08:00-09:00	Coffee & light breakfast
09:00-09:50	Theoretical Multiparty Computation Chair: Yehuda Lindell
	Adaptively Secure Garbling with Near Optimal Online Complexity Sanjam Garg, Akshayaram Srinivasan
	A New Approach to Black-Box Concurrent Secure Computation Sanjam Garg, Susumu Kiyoshima, Omkant Pandey
09:50-09:55	Track-switch break
09:55-10:45	Obfuscation Chair: Chris Brzuska
	Obfustopia Built on Secret-Key Functional Encryption Fuyuki Kitagawa, Ryo Nishimaki, Keisuke Tanaka
	Limits on Low-Degree Pseudorandom Generators (Or: Sum-of-Squares Meets Program Obfuscation) Boaz Barak, Zvika Brakerski, Ilan Komargodski, Pravesh K. Kothari
10:45-11:15	Coffee break
11:15-12:30	Zero-Knowledge Chair: Nir Bitansky
	On the Existence of Three Round Zero-Knowledge Proofs Nils Fleischhacker, Vipul Goyal, Abhishek Jain
	Statistical Witness Indistinguishability (and more) in Two Messages Yael Tauman Kalai, Dakshita Khurana, Amit Sahai
	An Efficiency-Preserving Transformation from Honest-Verifier Statistical Zero-Knowledge to Statistical Zero-Knowledge Pavel Hubáček, Alon Rosen, Margarita Vald

	Side hall (Israel C+D)
08:00-09:00	Coffee & light breakfast
09:00-09:50	Symmetric Cryptanalysis Chair: Itai Dinur
	Boomerang Connectivity Table: A New Cryptanalysis Tool Carlos Cid, Tao Huang, Thomas Peyrin, Yu Sasaki, Ling Song
	Correlation Cube Attacks: From Weak-Key Distinguisher to Key Recovery Meicheng Liu, Jingchun Yang, Wenhao Wang, Dongdai Lin
09:50-09:55	Track-switch break
09:55-10:45	Symmetric Cryptanalysis (Cont.) Chair: Yu Sasaki
	The Missing Difference Problem, and its Applications to Counter Mode Encryption Gaëtan Leurent, Ferdinand Sibleyras
	Fast Near Collision Attack on the Grain v1 Stream Cipher Bin Zhang, Chao Xu, Willi Meier
10:45-11:15	Coffee break
11:15-12:30	Implementing Multiparty Computation Chair: Eran Omri
	Efficient Maliciously Secure Multiparty Computation for RAM Marcel Keller, Avishay Yanai
	Efficient Circuit-based PSI via Cuckoo Hashing Benny Pinkas, Thomas Schneider, Christian Weinert, Udi Wieder
	Overdrive: Making SPDZ Great Again Marcel Keller, Valerio Pasto, Dragos Rotaru

	Main hall (Israel A)
12:30-14:00	Lunch
14:00-15:00	Eurocrypt 2018 Invited Talk Chair: Jesper Buus Nielsen
	Thirty Years of Digital Currency: From DigiCash to the Blockchain Matthew Green
15:00-15:30	Coffee Break
15:30-16:20	Non-Interactive Zero-Knowledge Chair: Moti Yung
	Efficient Designated-Verifier Non-Interactive Zero-Knowledge Proofs of Knowledge Pyrros Chaidos, Geoffroy Couteau
	Quasi-Optimal SNARGs via Linear Multi-Prover Interactive Proofs Dan Boneh, Yuval Ishai, Amit Sahai, David J. Wu
16:20-16:25	Track-switch break
16:25-17:45	IACR Membership Meeting

19:00-23:00	Banquet - Trask (Tel Aviv Port)
-------------	--

	Main hall (Israel A)
12:30-14:00	Lunch
14:00-15:00	Eurocrypt 2018 Invited Talk Main hall (Israel A) only
15:00-15:30	Coffee Break
15:30-16:20	Anonymous Communication Chair: Alon Rosen
	Untagging Tor: A Formal Treatment of Onion Encryption Jean Paul, Degabriele Martijn Stam
	Exploring the Boundaries of Topology Hiding Computation Marshall Ball, Elette Boyle, Tal Malkin, Tal Moran
16:20-16:25	Track-switch break
16:25-17:45	IACR Membership Meeting Main hall (Israel A) only

	Main hall (Israel A)
08:00-09:00	Coffee & light breakfast
09:00-09:25	Isogeny Chair: Wouter Castryck
	Supersingular Isogeny Graphs and Endomorphism Rings: Reductions and Solutions Kirsten Eisenträger, Sean Hallgren, Kristin Lauter, Travis Morrison, Christophe Petit
09:25-09:30	Track-switch break
09:55-10:45	Key Exchange Chair: Chris Brzuska
	Fuzzy Password-Authenticated Key Exchange Pierre-Alain Dupont, Julia Hesse, David Pointcheval, Leonid Reyzin, Sophia Yakubov
	Bloom Filter Encryption and Applications to Efficient Forward-Secret 0-RTT Key Exchange David Derler, Tibor Jager, Daniel Slamanig, Christoph Striecks
	OPAQUE: An Asymmetric PAKE Protocol Secure Against Pre-Computation Attacks Stanislaw Jarecki, Hugo Krawczyk, Jiayu Xu
10:45-11:15	Coffee break
11:15-12:05	Non-malleable Codes Chair: Moni Naor
	Non-malleable Randomness Encoders and their Applications Bhavana Kanukurthi, Sai Lakshmi Bhavana Obbattu, Sruthi Sekar
	Non-malleable Codes from Average-Case Hardness: AC^0, Decision Trees, and Streaming Space-Bounded Tampering Marshall Ball, Dana Dachman-Soled, Mukul Kulkarni, Tal Malkin
12:05-13:30	Lunch

	Side hall (Israel C+D)
08:30-09:30	Coffee & light breakfast
09:30-09:55	Leakage Chair: Olivier Pereira
	On the Complexity of Simulating Auxiliary Input Yi-Hsiu Chen, Kai-Min Chung, Jyun-Jie Liao
09:55-10:00	Track-switch break
10:00-11:15	Quantum Chair: Tanja Lange
	Unforgeable Quantum Encryption Gorjan Alagic, Tommaso Gagliardoni, Christian Majenz
	Tightly-Secure Key-Encapsulation Mechanism in the Quantum Random Oracle Model Tsunekazu Saito, Keita Xagawa, Takashi Yamakawa
	A Concrete Treatment of Fiat-Shamir Signatures in the Quantum Random-Oracle Model Eike Kiltz, Vadim Lyubashevsky, Christian Schaffner
11:15-11:45	Coffee break
11:45-12:35	Provable Symmetric Cryptography Chair: Christian Badertscher
	Naor-Reingold Goes Public: The Complexity of Known-key Security Pratik Soni, Stefano Tessaro
	Updatable Encryption with Post-Compromise Security Anja Lehmann, Björn Tackmann
12:35-14:00	Lunch