Hiroshi Fujiwara Cyber Security Research Center

PROGRAM | Monday | April 30, 2018

	Main hall (Israel A)	Side hall (Israel C+D)
08:00-09:00	Registration, coffee & light breakfast	Registration, coffee & light breakfast
09:00-09:10	**Opening Remarks** General Chair, Orr Dunkelman	**Opening Remarks** Main hall (Israel A) only
09:10-09:15	Track-switch break	Track-switch break
09:15-10:55	**Foundations** Chair: Alon Rosen	**Lattices** Chair: Muthuramakrishman Venkitasubramaniam
	On the Bit Security of Cryptographic Primitives Daniele Micciancio, Michael Walter	**Shortest Vector from Lattice Sieving: a Few Dimensions for Free** Léo Ducas
	On the Gold Standard for Security of Universal Steganography Sebastian Berndt, Maciej Liśkiewicz	**On the Ring-LWE and Polynomial-LWE problems** Miruna Rosca, Damien Stehlé, Alexandre Wallet
	Memory Lower Bounds of Reductions Revisited Yuyu Wang, Takahiro Matsuda, Goichiro Hanaoka, Keisuke Tanaka	**Faster Gaussian Sampling for Trapdoor Lattices with Arbitrary Modulus** Nicholas Genise, Daniele Micciancio
	Fiat-Shamir and Correlation Intractability from Strong KDM-Secure Encryption Ran Canetti, Yilei Chen, Leonid Reyzin, Ron D. Rothblum	**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	Coffee break
11:25-12:40	**Random Oracle Model** Chair: Yevgeniy Dodis	**Fully Homomorphic Encryption** Chair: Vinod Vaikuntanathan
	Random Oracles and Non-Uniformity Sandro Coretti, Yevgeniy Dodis, Siyao Guo, John P. Steinberger	**Homomorphic Lower Digits Removal and Improved FHE Bootstrapping** Hao Chen, Kyoohyung Han
	Another Step Towards Realizing Random Oracles: Non-Malleable Point Obfuscation Ilan Komargodski, Eylon Yogev	**Homomorphic SIM^{2}D Operations: Single Instruction Much More Data** Wouter Castryck, Ilia Iliashenko, Frederik Vercauteren
	The Wonderful World of Global Random Oracles Jan Camenisch, Manu Drijvers, Tommaso Gagliardoni, Anja Lehmann, Gregory Neven	**Bootstrapping for Approximate Homomorphic Encryption** Jung Hee Cheon, Kyoohyung Han, Andrey Kim, Miran Kim, Yongsoo Song
12:40-14:10	Lunch	Lunch
14:10-15:10	**Invited Talk** Chair: Vincent Rijmen	**Invited Talk** Main hall (Israel A) only
	Desperately Seeking Sboxes Anne Canteaut	
15:10-15:40	Coffee break	Coffee break
15:40-16:30	**Permutations** Chair: Bart Preneel	**Attribute-Based Encryption** Chair: Carmit Hazay
	Full Indifferentiable Security of the Xor of Two or More Random Permutations Using the X^2 Method Srimanta Bhattacharya, Mridul Nandi	**Unbounded ABE via Bilinear Entropy Expansion, Revisited** Jie Chen, Junqing Gong, Lucas Kowalczyk, Hoeteck Wee
	An Improved Affine Equivalence Algorithm for Random Permutations Itai Dinur	**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	Track-switch break
16:35-17:25	**Galois Counter Mode** Chair: Tomer Ashur	**Secret Sharing** Chair: Yuval Ishai
	Optimal Forgeries Against Polynomial-Based MACs and GCM Atul Luykx, Bart Preneel	**Towards Breaking the Exponential Barrier for General Secret Sharing** Tianren Liu, Vinod Vaikuntanathan, Hoeteck Wee
	Revisiting AES-GCM-SIV: Multi-user Security, Faster Key Derivation, and Better Bounds Priyanka Bose, Viet Tung Hoang, Stefano Tessaro	**Improving the Linear Programming Technique in the Search for Lower Bounds in Secret Sharing** Oriol Farràs, Tarik Kaced, Sebastià Martín, Carles Padró

Hiroshi Fujiwara Cyber Security Research Center

PROGRAM | Tuesday | May 1, 2018

	Main hall (Israel A)	Side hall (Israel C+D)
08:00-09:00	Coffee & light breakfast	Coffee & light breakfast
09:00-09:50	**Blockchain** Chair: Ivan Visconti	**Multi-Collision Resistance** Chair: Jens Groth
	Thunderella: Blockchains with Optimistic Instant Confirmation Rafael Pass, Elaine Shi	**Multi-Collision Resistant Hash Functions and their Applications** Itay Berman, Akshay Degwekar, Ron D. Rothblum, Prashant Nalini Vasudevan
	But Why Does it Work? A Rational Protocol Design Treatment of Bitcoin Christian Badertscher, Juan A. Garay, Ueli Maurer, Daniel Tschudi, Vassilis Zikas	**Collision Resistant Hashing for Paranoids: Dealing with Multiple Collisions** Ilan Komargodski, Moni Naor, Eylon Yogev
09:50-09:55	Track-switch break	Track-switch break
09:55-10:45	**Blockchain (Cont.)** Chair: Ivan Visconti	**Signatures** Chair: Jens Groth
	Ouroboros Praos: An adaptively-secure, semi-synchronous proof-of-stake blockchain Bernardo David, Peter Gaži, Aggelos Kiayias, Alexander Russell	**Synchronized Aggregate Signatures from the RSA Assumption** Susan Hohenberger, Brent Waters
	Sustained Space Complexity Joël Alwen, Jeremiah Blocki, Krzysztof Pietrzak	**More Efficient (Almost) Tightly Secure Structure-Preserving Signatures** Romain Gay, Dennis Hofheinz, Lisa Kohl, Jiaxin Pan
10:45-11:15	Coffee break	Coffee break
11:15-12:30	**Privte Simultaneous Massages** Chair: Yuval Ishai	**Masking** Chair: Gaëtan Leurent
	The Communication Complexity of Private Simultaneous Messages, Revisited Benny Applebaum, Thomas Holenstein, Manoj Mishra, Ofer Shayevitz	**Formal Verification of Masked Hardware Implementations in the Presence of Glitches** Roderick Bloem, Hannes Gross, Rinat Iusupov, Bettina Könighofer, Stefan Mangard, Johannes Winter
	The Complexity of Multiparty PSM Protocols and Related Models Amos Beimel, Eyal Kushilevitz, Pnina Nissim	**Masking the GLP Lattice-Based Signature Scheme at Any Order** Gilles Barthe, Sonia Belaïd, 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
12:30-14:00	Lunch	
14:00-14:25	**Best Young Research Award - Main hall (Israel A)** Chair: Eike Kiltz	
	The Discrete-Logarithm Problem with Preprocessing Henry Corrigan-Gibbs, Dmitry Kogan	
14:25-15:40	**Best Paper Awards - Main hall (Israel A)** 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) Chairs: Daniel J. Bernstein and Tanja Lange
18:30-19:30	Rump Session Reception
19:30-21:00	**Rump Session**
21:00-21:30	Break
21:30-23:00	**Rump Session (Cont.)**

Hiroshi Fujiwara Cyber Security Research Center

PROGRAM | Wednesday | May 2, 2018

	Main hall (Israel A)	Side hall (Israel C+D)
08:00-09:00	Coffee & light breakfast	Coffee & light breakfast
09:00-09:50	**Theoretical Multiparty Computation** Chair: Yehuda Lindell	**Symmetric Cryptanalysis** Chair: Itai Dinur
	Adaptively Secure Garbling with Near Optimal Online Complexity Sanjam Garg, Akshayaram Srinivasan	**Boomerang Connectivity Table: A New Cryptanalysis Tool** Carlos Cid, Tao Huang, Thomas Peyrin, Yu Sasaki, Ling Song
	A New Approach to Black-Box Concurrent Secure Computation Sanjam Garg, Susumu Kiyoshima, Omkant Pandey	**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	Track-switch break
09:55-10:45	**Obfuscation** Chair: Chris Brzuska	**Symmetric Cryptanalysis (Cont.)** Chair: Yu Sasaki
	Obfustopia Built on Secret-Key Functional Encryption Fuyuki Kitagawa, Ryo Nishimaki, Keisuke Tanaka	**The Missing Difference Problem, and its Applications to Counter Mode Encryption** Gaëtan Leurent, Ferdinand Sibleyras
	Limits on Low-Degree Pseudorandom Generators (Or: Sum-of-Squares Meets Program Obfuscation) Boaz Barak, Zvika Brakerski, Ilan Komargodski, Pravesh K. Kothari	**Fast Near Collision Attack on the Grain v1 Stream Cipher** Bin Zhang, Chao Xu, Willi Meier
10:45-11:15	Coffee break	Coffee break
11:15-12:30	**Zero-Knowledge** Chair: Nir Bitansky	**Implementing Multiparty Computation** Chair: Eran Omri
	On the Existence of Three Round Zero-Knowledge Proofs Nils Fleischhacker, Vipul Goyal, Abhishek Jain	**Efficient Maliciously Secure Multiparty Computation for RAM** Marcel Keller, Avishay Yanai
	Statistical Witness Indistinguishability (and more) in Two Messages Yael Tauman Kalai, Dakshita Khurana, Amit Sahai	**Efficient Circuit-based PSI via Cuckoo Hashing** Benny Pinkas, Thomas Schneider, Christian Weinert, Udi Wieder
	An Efficiency-Preserving Transformation from Honest-Verifier Statistical Zero-Knowledge to Statistical Zero-Knowledge Pavel Hubáček, Alon Rosen, Margarita Vald	**Overdrive: Making SPDZ Great Again** Marcel Keller, Valerio Pastro, Dragos Rotaru
12:30-14:00	Lunch	Lunch
14:00-15:00	**Eurocrypt 2018 Invited Talk** Chair: Jesper Buus Nielsen	**Eurocrypt 2018 Invited Talk** Main hall (Israel A) only
	Thirty Years of Digital Currency: From DigiCash to the Blockchain Matthew Green	
15:00-15:30	Coffee Break	Coffee Break
15:30-16:20	**Non-Interactive Zero-Knowledge** Chair: Moti Yung	**Anonymous Communication** Chair: Alon Rosen
	Efficient Designated-Verifier Non-Interactive Zero-Knowledge Proofs of Knowledge Pyrros Chaidos, Geoffroy Couteau	**Untagging Tor: A Formal Treatment of Onion Encryption** Jean Paul, Degabriele Martijn Stam
	Quasi-Optimal SNARGs via Linear Multi-Prover Interactive Proofs Dan Boneh, Yuval Ishai, Amit Sahai, David J. Wu	**Exploring the Boundaries of Topology Hiding Computation** Marshall Ball, Elette Boyle, Tal Malkin, Tal Moran
16:20-16:25	Track-switch break	Track-switch break
16:25-17:45	**IACR Membership Meeting**	**IACR Membership Meeting** Main hall (Israel A) only
19:00-23:00	**Banquet - Trask (Tel Aviv Port)**	

Hiroshi Fujiwara Cyber Security Research Center

PROGRAM | Thursday | May 3, 2018

	Main hall (Israel A)	Side hall (Israel C+D)
08:30-09:30	Coffee & light breakfast	Coffee & light breakfast
09:30-09:55	**Isogeny** Chair: Wouter Castryck	**Leakage** Chair: Olivier Pereira
	Supersingular Isogeny Graphs and Endomorphism Rings: Reductions and Solutions Kirsten Eisenträger, Sean Hallgren, Kristin Lauter, Travis Morrison, Christophe Petit	**On the Complexity of Simulating Auxiliary Input** Yi-Hsiu Chen, Kai-Min Chung, Jyun-Jie Liao
09:55-10:00	Track-switch break	Track-switch break
10:00-11:15	**Key Exchange** Chair: Chris Brzuska	**Quantum** Chair: Tanja Lange
	Fuzzy Password-Authenticated Key Exchange Pierre-Alain Dupont, Julia Hesse, David Pointcheval, Leonid Reyzin, Sophia Yakoubov	**Unforgeable Quantum Encryption** Gorjan Alagic, Tommaso Gagliardoni, Christian Majenz
	Bloom Filter Encryption and Applications to Efficient Forward-Secret 0-RTT Key Exchange David Derler, Tibor Jager, Daniel Slamanig, Christoph Striecks	**Tightly-Secure Key-Encapsulation Mechanism in the Quantum Random Oracle Model** Tsunekazu Saito, Keita Xagawa, Takashi Yamakawa
	OPAQUE: An Asymmetric PAKE Protocol Secure Against Pre-Computation Attacks Stanislaw Jarecki, Hugo Krawczyk, Jiayu Xu	**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	Coffee break
11:45-12:35	**Non-malleable Codes** Chair: Moni Naor	**Provable Symmetric Cryptography** Chair: Christian Badertscher
	Non-malleable Randomness Encoders and their Applications Bhavana Kanukurthi, Sai Lakshmi Bhavana Obbattu, Sruthi Sekar	**Naor-Reingold Goes Public: The Complexity of Known-key Security** Pratik Soni, Stefano Tessaro
	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	**Updatable Encryption with Post-Compromise Security** Anja Lehmann, Björn Tackmann
12:35-14:00	Lunch	Lunch