Crypto 2018 Program

Sunday, August 19, 2018

17:00–20:00	**Registration** Location: Anacapa Formal Lounge
17:30–21:30	**Reception Dinner** Location: Anacapa Lawn

Monday, August 20, 2018

7:30–8:45	**Breakfast** Location: De La Guerra Dining Commons	
8:50–9:00	**Opening remarks** Location: Corwin Pavilion Chair: Crypto General Chair, Tal Rabin	
9:05–10:25	**Secure Messaging** Location: Lotte Lehman Hall Chair: Kenny Paterson **Towards Bidirectional Ratcheted Key Exchange** Bertram Poettering, Paul Rösler *Royal Holloway, University of London, Ruhr University Bochum* **Optimal Channel Security Against Fine-Grained State Compromise: The Safety of Messaging** Joseph Jaeger, Igors Stepanovs *UC San Diego* **Out-of-Band Authentication in Group Messaging: Computational, Statistical, Optimal** Lior Rotem, Gil Segev *Hebrew University of Jerusalem*	**Round Optimal MPC** Location: Corwin Pavilion Chair: Fabrice Benhamouda **Round-Optimal Secure Multiparty Computation with Honest Majority** Prabhanjan Ananth, Arka Rai Choudhuri, Aarushi Goel, Abhishek Jain *MIT, JHU* **On the Exact Round Complexity of Secure Three-Party Computation** Arpita Patra, Divya Ravi *Indian Institute of Science, India* **Soft Merge with the next talk: Promise Zero Knowledge and its Applications to Round Optimal MPC** Saikrishna Badrinarayanan, Vipul Goyal, Abhishek Jain, Yael Tauman Kalai, Dakshita Khurana, Amit Sahai *UCLA, CMU, JHU, MIT and Microsoft Research* **Round-Optimal Secure Multi-Party Computation** Shai Halevi, Carmit Hazay, Antigoni Polychroniadou, Muthuramakrishnan Venkitasubramaniam *IBM, Bar Ilan University, Cornell-Tech / University of Rochester, University of Rochester*
10:20–10:50	**Coffee Break**	
10:50–11:40	**Implementations and Physical Attacks** Location: Lotte Lehman Hall Chair: Tancrède Lepoint **Faster Homomorphic Linear Transformations in HElib** Shai Halevi, Victor Shoup *IBM Research, NYU* **CAPA: The Spirit of Beaver against Physical Attacks** Oscar Reparaz, Lauren De Meyer, Begül Bilgin, Victor Arribas, Svetla Nikova, Ventzislav Nikov, Nigel P. Smart *KU Leuven, imec - Cosic, Leuven, Belgium, Square Inc., San Francisco, USA, NXP Semiconductors, Leuven, Belgium*	**Foundations** Location: Corwin Pavilion Chair: Daniel Wichs **Yes, There is an Oblivious RAM Lower Bound!** Kasper Green Larsen, Jesper Buus Nielsen *Aarhus University* **Constrained PRFs for NC1 in Traditional Groups** Nuttapong Attrapadung, Takahiro Matsuda, Ryo Nishimaki, Shota Yamada, Takashi Yamakawa *AIST, NTT Secure Platform Laboratories*
11:40–11:45	**Track-switch Break**	

Monday, August 20, 2018

11:45–12:45

IACR Distinguished Lecture

Location: Corwin Pavilion
Chair: Tal Rabin

From Idea to Impact, the Crypto story: What's next?
Shafi Goldwasser
Berkeley and MIT

12:50–14:00

Lunch

Location: De La Guerra Dining Commons

14:15–15:30

Authenticated and Format-Preserving Encryption

Location: Lotte Lehman Hall
Chair: Aishwarya Thiruvengadam

Fast Message Franking: From Invisible Salamanders to Encryptment
Yevgeniy Dodis, Paul Grubbs, Thomas Ristenpart, Joanne Woodage
NYU, Cornell Tech, Royal Holloway

Indifferentiable Authenticated Encryption
Manuel Barbosa, Pooya Farshim
INESC TEC and FC University of Porto, DI/ENS, CNRS, PSL University and Inria, Paris, France

The Curse of Small Domains: New Attacks on Format-Preserving Encryption
Viet Tung Hoang, Stefano Tessaro, Ni Trieu
Florida State University, UCSB, Oregon State University

Lattices

Location: Corwin Pavilion
Chair: Daniele Micciancio

GGH15 Beyond Permutation Branching Programs: Proofs, Attacks, and Candidates
Yilei Chen, Vinod Vaikuntanathan, Hoeteck Wee
Boston University, MIT, CNRS and ENS, PSL

Lower Bounds on Lattice Enumeration with Extreme Pruning
Yoshinori Aono, Phong Q. Nguyen, Takenobu Seito, Junji Shikata
NICT, Inria and CNRS, JFLI, University of Tokyo, Bank of Japan, Yokohama National University

Dissection-BKW
Andre Esser, Felix Heuer, Robert Kübler, Alexander May, Christian Sohler
Ruhr University Bochum, TU Dortmund

15:30–16:00

Coffee Break

16:00–17:15

Cryptanalysis

Location: Lotte Lehman Hall
Chair: Viet Tung Hoang

Cryptanalysis via algebraic spans
Adi Ben-Zvi, Arkadius Kalka, Boaz Tsaban
Bar-Ilan University

Improved Division Property Based Cube Attacks Exploiting Algebraic Properties of Superpoly
Qingju Wang, Yonglin Hao, Yosuke Todo, Chaoyun Li, Takanori Isobe, Willi Meier
University of Luxembourg, Luxembourg, State Key Laboratory of Cryptology, P.O. Box 5159, Beijing 100878, China, NTT Secure Platform Laboratories, Japan, imec-COSIC, Dept. Electrical Engineering (ESAT), KU Leuven, Belgium, University of Hyogo, Japan, FHNW, Switzerland

Generic Attacks against Beyond-Birthday-Bound MACs
Gaëtan Leurent, Mridul Nandi, Ferdinand Sibleyras
Inria,

Lattice-based Zero Knowledge

Location: Corwin Pavilion
Chair: Anna Lysyanskaya

Sub-Linear Lattice-Based Zero-Knowledge Arguments for Arithmetic Circuits
Carsten Baum, Jonathan Bootle, Andrea Cerulli, Rafael del Pino, Jens Groth, Vadim Lyubashevsky
Bar Ilan University, UCL, IBM Research - Zurich

Lattice-Based Zero-Knowledge Arguments for Integer Relations
Benoît Libert, San Ling, Khoa Nguyen, Huaxiong Wang
CNRS and ENS de Lyon (France), Nanyang Technological University (Singapore)

Multi-Theorem Preprocessing NIZKs from Lattices
Sam Kim, David J. Wu
Stanford University

19:00–21:00

Dinner

Location: Anacapa Lawn

Tuesday, August 21, 2018

7:30–8:35

Breakfast

Location: De La Guerra Dining Commons

Tuesday, August 21, 2018

8:40–10:20

Searchable Encryption and Differential Privacy

Location: Lotte Lehman Hall - starts at 8:55
Chair: Alexandra Boldyreva

Structured Encryption and Leakage Suppression
Seny Kamara, Tarik Moataz, Olga Ohrimenko
Brown University, Microsoft Research

Soft Merge with the next talk: Searchable Encryption with Optimal Locality: Achieving Sublogarithmic Read Efficiency
Ioannis Demertzis, Dimitrios Papadopoulos, Charalampos Papamanthou
University of Maryland, Hong Kong University of Science and Technology

Tight Tradeoffs in Searchable Symmetric Encryption
Gilad Asharov, Gil Segev, Ido Shahaf
Cornell Tech, Hebrew University of Jerusalem

Soft Merge with the next talk: Hardness of Non-Interactive Differential Privacy from One-Way Functions
Lucas Kowalczyk, Tal Malkin, Jonathan Ullman, Daniel Wichs
Columbia University, Northeastern University

Risky Traitor Tracing and New Differential Privacy Negative Results
Rishab Goyal, Venkata Koppula, Andrew Russell, Brent Waters
UT Austin

Efficient MPC

Location: Corwin Pavilion
Chair: Mike Rosulek

SPDZ2k: Efficient MPC mod 2^k for Dishonest Majority
Ronald Cramer, Ivan Damgård, Daniel Escudero, Peter Scholl, Chaoping Xing
CWI, Amsterdam, Aarhus University, Aarhus Univerity, Nanyang Technological University, Singapore

Yet Another Compiler for Active Security or: Efficient MPC Over Arbitrary Rings
Ivan Damgård, Claudio Orlandi, Mark Simkin
Aarhus University

TinyKeys: A New Approach to Efficient Multi-Party Computation
Carmit Hazay, Emmanuela Orsini, Peter Scholl, Eduardo Soria-Vazquez
Bar-Ilan University, KU Leuven, Aarhus University, University of Bristol

Fast Large-Scale Honest-Majority MPC for Malicious Adversaries
Koji Chida, Daniel Genkin, Koki Hamada, Dai Ikarashi, Ryo Kikuchi, Yehuda Lindell, Ariel Nof
NTT Secure Platform Laboratories, University of Pennsylvania and University of Maryland, Bar-Ilan University

10:20–10:50 — **Coffee Break**

10:50–11:40

Secret Sharing

Location: Lotte Lehman Hall
Chair: Hoeteck Wee

Non-Malleable Secret Sharing for General Access Structures
Vipul Goyal, Ashutosh Kumar
CMU, UCLA

On the Local Leakage Resilience of Linear Secret Sharing Schemes
Fabrice Benhamouda, Akshay Degwekar, Yuval Ishai, Tal Rabin
IBM Research, MIT, Technion

Quantum Cryptography I

Location: Corwin Pavilion
Chair: Alexandra Boldyreva

Quantum FHE (Almost) As Secure As Classical
Zvika Brakerski
Weizmann Institute of Science

IND-CCA-secure Key Encapsulation Mechanism in the Quantum Random Oracle Model, Revisited
Haodong Jiang, Zhenfeng Zhang, Long Chen, Hong Wang, Zhi Ma
State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou, Henan, China, TCA Laboratory, State Key Laboratory of Computer Science, Institute of Software, Chinese Academy of Sciences, China, TCA Laboratory, State Key Laboratory of Computer Science, Institute of Software, Chinese Academy of Sciences, China, University of Chinese Academy of Sciences, Beijing, China, State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou, Henan, China, State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou, Henan, China, CAS Center for Excellence and Synergetic Innovation Center in Quantum information and Quantum Physics,USTC, Hefei, Anhui, China

11:40–11:45 — **Track-switch Break**

Tuesday, August 21, 2018

11:45–12:40

Encryption

Location: Lotte Lehman Hall
Chair: Ananth Raghunathan

Threshold Cryptosystems From Threshold Fully Homomorphic Encryption
Dan Boneh, Rosario Gennaro, Steven Goldfeder, Aayush Jain, Sam Kim, Peter M. R. Rasmussen, Amit Sahai
Stanford University, City College of New York, Princeton University, UCLA and Center for Encrypted Functionalities

Multi-Input Functional Encryption for Inner Products: Function-Hiding Realizations and Constructions without Pairings
Michel Abdalla, Dario Catalano, Dario Fiore, Romain Gay, Bogdan Ursu
Departement informatique de l'ENS, Ecole normale supérieure, CNRS, PSL University, 75005 Paris, France and INRIA, Paris, France, Università di Catania, Italy, IMDEA Software Institute, Madrid, Spain, KIT, Karlsruhe, Germany

Quantum Cryptography II

Location: Corwin Pavilion
Chair: Chitchanok Chuengsatiansup

Pseudorandom Quantum States
Zhengfeng Ji, Yi-Kai Liu, Fang Song
University of Technology Sydney, University of Maryland and NIST, Portland State University

Soft Merge with the next talk: Quantum Attacks against Indistinguishablility Obfuscators Proved Secure in the Weak Multilinear Map Model
Alice Pellet-Mary
Univ Lyon, CNRS, ENS de Lyon, Inria, UCBL, LIP, Lyon, France.

Cryptanalyses of Branching Program Obfuscations over GGH13 Multilinear Map from the NTRU Problem
Jung Hee Cheon, Minki Hhan, Jiseung Kim, Changmin Lee
Seoul National University

12:45–14:00 — **Lunch**
Location: De La Guerra Dining Commons

14:00–18:00 — **Free afternoon**

18:00–21:00 — **Dinner Reception**
Location: University Center Lagoon Plaza

19:00–19:30 — **IACR Award Ceremony**
Location: Corwin Pavilion

19:30–23:00 — **Rump Session**
Location: Corwin Pavilion
Chair: Stuart Haber

Wednesday, August 22, 2018

7:30–8:35 — **Breakfast**
Location: De La Guerra Dining Commons

Wednesday, August 22, 2018

8:40–10:20

Symmetric Cryptography

Location: Lotte Lehman Hall
Chair: Xuejia Lai

Encrypt or Decrypt? To Make a Single-Key Beyond Birthday Secure Nonce-Based MAC
Nilanjan Datta, Avijit Dutta, Mridul Nandi, Kan Yasuda
Indian Institute of Technology, Kharagpur, Indian Statistical Institute, Kolkata, NTT Information Sharing Platform Laboratories, NTT Corporation, Japan

Rasta: A cipher with low ANDdepth and few ANDs per bit
Christoph Dobraunig, Maria Eichlseder, Lorenzo Grassi, Virginie Lallemand, Gregor Leander, Eik List, Florian Mendel, Christian Rechberger
Graz University of Technology, Horst Görtz Institute for IT Security, Ruhr-Universität Bochum, Bauhaus-Universität Weimar, Infineon Technologies AG

Non-Uniform Bounds in the Random-Permutation, Ideal-Cipher, and Generic-Group Models
Sandro Coretti, Yevgeniy Dodis, Siyao Guo
New York University, Northeastern University

Provable Security of (Tweakable) Block Ciphers Based on Substitution-Permutation Networks
Benoit Cogliati, Yevgeniy Dodis, Jonathan Katz, Jooyoung Lee, John Steinberger, Aishwarya Thiruvengadam, Zhe Zhang
University of Luxembourg, Luxembourg, New York University, USA, University of Maryland, USA, KAIST, Korea, , University of California, Santa Barbara, Tsinghua University, Beijing

MPC

Location: Corwin Pavilion
Chair: Seny Kamara

An Optimal Distributed Discrete Log Protocol with Applications to Homomorphic Secret Sharing
Itai Dinur, Nathan Keller, Ohad Klein
Ben-Gurion University, Israel, Bar-Ilan University, Israel

Must the Communication Graph of MPC Protocols be an Expander?
Elette Boyle, Ran Cohen, Deepesh Data, Pavel Hubacek
IDC Herzliya, MIT and Northeastern University, UCLA, Charles University

Two-Round Multiparty Secure Computation Minimizing Public Key Operations
Sanjam Garg, Peihan Miao, Akshayaram Srinivasan
University of California, Berkeley

Limits of Practical Sublinear Secure Computation
Elette Boyle, Yuval Ishai, Antigoni Polychroniadou
IDC Herzliya, Technion, Cornell Tech and University of Rochester

10:20–10:50 — **Coffee Break**

10:50–11:40

Proofs of Work and Proofs of Stake

Location: Lotte Lehman Hall
Chair: Alessandra Scafuro

Verifiable Delay Functions
Dan Boneh, Joseph Bonneau, Benedikt Bünz, Ben Fisch
Stanford University, New-York University

Proofs of Work from Worst-Case Assumptions
Marshall Ball, Alon Rosen, Manuel Sabin, Prashant Nalini Vasudevan
Columbia University, IDC Herzliya, UC Berkeley, MIT

Garbling

Location: Corwin Pavilion
Chair: Hoeteck Wee

Limits on the Power of Garbling Techniques for Public-Key Encryption
Sanjam Garg, Mohammad Hajiabadi, Mohammad Mahmoody, Ameer Mohammed
University of California, Berkeley,

Optimizing Authenticated Garbling for Faster Secure Two-Party Computation
Jonathan Katz, Samuel Ranellucci, Mike Rosulek, Xiao Wang
University of Maryland, University of Maryland and George Mason University, Oregon State University

11:40–11:45 — **Track-switch Break**

11:45–12:45

Invited Talk

Location: Corwin Pavillon
Chair: Hovav Shacham

Crypto: a Key Ingredient to Building Respectful Products
Lea Kissner
Google

12:50–14:00

Lunch

Location: De La Guerra Dining Commons

Wednesday, August 22, 2018

14:15–15:05

Proof Tools

Location: Lotte Lehman Hall
Chair: Alexandra Boldyreva

Simplifying Game-Based Definitions: Indistinguishability up to Correctness and Its Application to Stateful AE
Phillip Rogaway, Yusi Zhang
University of California, Davis, USA

The Algebraic Group Model and its Applications
Georg Fuchsbauer, Eike Kiltz, Julian Loss
Inria, ENS, CNRS, PSL, France, Ruhr University Bochum, Germany

Information-Theoretic MPC

Location: Corwin Pavilion
Chair: Daniel Wichs

Amortized Complexity of Information-Theoretically Secure MPC Revisited
Ignacio Cascudo, Ronald Cramer, Chaoping Xing, Chen Yuan
Aalborg University, Denmark, CWI Amsterdam and Leiden University, the Netherlands, Nanyang Technological University, Singapore, CWI Amsterdam, the Netherlands

Private Circuits: A Modular Approach
Prabhanjan Ananth, Yuval Ishai, Amit Sahai
MIT, Technion, UCLA

15:05–15:35 — **Coffee Break**

15:35–16:25

Key Exchange

Location: Lotte Lehman Hall
Chair: Marc Fischlin

On Tightly Secure Non-Interactive Key Exchange
Julia Hesse, Dennis Hofheinz, Lisa Kohl
TU Darmstadt, Karlsruhe Institute of Technology

Practical and Tightly-Secure Digital Signatures and Authenticated Key Exchange
Kristian Gjøsteen, Tibor Jager
NTNU - Norwegian University of Science and Technology, Trondheim, Norway, Paderborn University, Paderborn, Germany

Various Topics

Location: Corwin Pavilion
Chair: Hoeteck Wee

A New Public-Key Cryptosystem via Mersenne Numbers
Divesh Aggarwal, Antoine Joux, Anupam Prakash, Miklos Santha
NUS, Fondation Partenariale de l, NTU and CQT, NUS, CNRS and CQT, NUS

Fast Homomorphic Evaluation of Deep Discretized Neural Networks
Florian Bourse, Michele Minelli, Matthias Minihold, Pascal Paillier
Orange Labs, ENS, CNRS, PSL Research University, Inria, Ruhr-Universität Bochum, CryptoExperts

16:35–17:35 — **IACR Membership Meeting**
Location: Corwin Pavilion

18:00–19:30 — **Beach Barbeque**
Location: Goleta Beach

19:30–22:30 — **Crypto Café**
Location: Anacapa Formal Lounge and Anacapa Front Lawn

Thursday, August 23, 2018

7:30–8:35 — **Breakfast**
Location: De La Guerra Dining Commons

Thursday, August 23, 2018

8:40–10:20

Symmetric Cryptanalysis

Location: Lotte Lehman Hall
Chair: Hovav Shacham

Improved Key Recovery Attacks on Reduced-Round AES with Practical Data and Memory Complexities
Achiya Bar-On, Orr Dunkelman, Nathan Keller, Eyal Ronen, Adi Shamir
Bar Ilan University, Israel, University of Haifa, Israel, Weizmann Institute, Israel

Fast Correlation Attack Revisited - Cryptanalysis on Full Grain-128a, Grain-128, and Grain-v1
Yosuke Todo, Takanori Isobe, Willi Meier, Kazumaro Aoki, Bin Zhang
NTT Secure Platform Laboratories, University of Hyogo, FHNW, Chinese Academy of Sciences

A Key-recovery Attack on 855-round Trivium
Ximing Fu, Xiaoyun Wang, Xiaoyang Dong, Willi Meier
Tsinghua University, Tsinghua University, Shandong University, FHNW

Bernstein Bound on WCS is Tight - Repairing Luykx-Preneel Optimal Forgeries
Mridul Nandi
Indian Statistical Institute, Kolkata

Oblivious Transfer and Non-Malleable Codes

Location: Corwin Pavilion
Chair: Pooya Farshim

Adaptive Garbled RAM from Laconic Oblivious Transfer
Sanjam Garg, Rafail Ostrovsky, Akshayaram Srinivasan
University of California, Berkeley, UCLA

On the Round Complexity of OT Extension
Sanjam Garg, Mohammad mahmoody, Daniel Masny, Izaak Meckler
Berkeley, University of Virginia

Non-Malleable Codes for Partial Functions with Manipulation Detection
Aggelos Kiayias, Feng-Hao Liu, Yiannis Tselekounis
University of Edinburgh, Florida Atlantic University

Continuously Non-Malleable Codes in the Split-State Model from Minimal Assumptions
Rafail Ostrovsky, Giuseppe Persiano, Daniele Venturi, Ivan Visconti
UCLA, University of Salerno, Sapienza University of Rome

10:20–10:50 — **Coffee Break**

10:50–12:05

Hashes and Random Oracles

Location: Lotte Lehman Hall
Chair: Stanislaw Jarecki

Correcting Subverted Random Oracles
Alexander Russell, Qiang Tang, Moti Yung, Hong-Sheng Zhou
UNIVERSITY OF CONNECTICUT, New Jersey Institute of Technology, Snapchat and Columbia University, Virginia Commonwealth University

Combiners for Backdoored Random Oracles
Balthazar Bauer, Pooya Farshim, Sogol Mazaheri
École Normale Supérieure, Technische Universität Darmstadt

On Distributional Collision Resistant Hashing
Ilan Komargodski, Eylon Yogev
Cornell Tech, Weizmann Institute

Zero Knowledge

Location: Corwin Pavilion
Chair: Daniel Genkin

Non-Interactive Zero-Knowledge Proofs for Composite Statements
Shashank Agrawal, Chaya Ganesh, Payman Mohassel
Visa Research, Aarhus University

From Laconic Zero-Knowledge to Public-Key Cryptography
Itay Berman, Akshay Degwekar, Ron D. Rothblum, Prashant Nalini Vasudevan
MIT, MIT, Northeastern University

Updatable and Universal Common Reference Strings with Applications to zk-SNARKs
Jens Groth, Markulf Kohlweiss, Mary Maller, Sarah Meiklejohn, Ian Miers
University College London, University of Edinburgh, Cornell Tech

12:05–12:10 — **Track-switch Break**

Thursday, August 23, 2018		
12:10–13:00	**Trapdoor Functions** Location: Lotte Lehman Hall Chair: Marc Fischlin **Fast Distributed RSA Key Generation for Semi-Honest and Malicious Adversaries** Tore K. Frederiksen, Yehuda Lindell, Valery Osheter, Benny Pinkas *Alexandra Institute, Bar-Ilan University, Unbound Tech Ltd.* **Trapdoor Functions from the Computational Diffie-Hellman Assumption** Sanjam Garg, Mohammad Hajiabadi *University of California Berkeley, University of California Berkeley and University of Virginia*	**Obfuscation** Location: Corwin Pavilion Chair: Tancrède Lepoint **On the Complexity of Compressing Obfuscation** Gilad Asharov, Naomi Ephraim, Ilan Komargodski, Rafael Pass *Cornell Tech, Cornell University* **A Simple Obfuscation Scheme for Pattern-Matching with Wildcards** Allison Bishop, Lucas Kowalczyk, Tal Malkin, Valerio Pastro, Mariana Raykova, Kevin Shi *IEX, Columbia University, Columbia University, Columbia University, Yale University, Yale University*
13:05–14:00	**Lunch** Location: De La Guerra Dining Commons	