TCC 2017

15^{th} IACR Theory of Cryptography Conference

https://www.iacr.org/workshops/tcc2017/

Handbook

November 12^{th}-15^{th}, 2017
Baltimore, USA

Program Chairs

Yael Kalai (Microsoft Research New England)
Leonid Reyzin (Boston University)

General Chair

Abhishek Jain (Johns Hopkins University)

Organizing Committee

Arka Rai Choudhuri (Johns Hopkins University)
Anton Dahbura (Johns Hopkins University)
Jessica Finkelstein (Johns Hopkins University)
Nils Fleischhacker (Johns Hopkins University)
Aarushi Goel (Johns Hopkins University)
Zhengzhong Jin (Johns Hopkins University)
Revelie Niles (Johns Hopkins University)

Platinum Sponsors

JOHNS HOPKINS WHITING SCHOOL of ENGINEERING | Information Security Institute

JOHNS HOPKINS WHITING SCHOOL of ENGINEERING
Department of Computer Science

Gold Sponsors

IBM

Microsoft Research

Silver Sponsors

Google

Program

	Sunday, November 12 (Johns Hopkins Club)
17:30-18:00	Registration
18:00-20:00	Welcome Reception

	Monday, November 13 (Charles Commons Conference Center)
08:55-09:00	Opening Remarks
	Obfuscation
09:00-09:20	**Limits on the Locality of Pseudorandom Generators (with Applications to Indistinguishability Obfuscation)** Alex Lombardi and Vinod Vaikuntanathan
09:20-09:40	**Decomposable Obfuscation: A Framework for Building Applications of Obfuscation From Polynomial Hardness** Qipeng Liu and Mark Zhandry
	Functional Encryption
09:40-10:00	**Functional Encryption for Bounded Collusions, Revisited** Shweta Agrawal and Alon Rosen
10:00-10:20	Attribute-Hiding Predicate Encryption in Bilinear Groups, Revisited Hoeteck Wee
10:20-10:50	Coffee Break
	Obfuscation and Functional Encryption
10:50-11:10	**When does Functional Encryption Imply Obfuscation?** Sanjam Garg, Mohammad Mahmoody, and Ameer Mohammed
	Delegation
11:10-11:30	**On Zero-Testable Homomorphic Encryption and Publicly Verifiable Non-Interactive Arguments** Omer Paneth and Guy N. Rothblum
	Constrained PRFs
11:30-11:50	**Private Constrained PRFs (and more) from LWE** Zvika Brakerski, Rotem Tsabary, Vinod Vaikuntanathan, and Hoeteck Wee
11:50-12:10	**Constrained Keys For Invertible Pseudorandom Functions** Dan Boneh, Sam Kim, and David J. Wu
12:10-13:30	Lunch
	Databases
13:30-13:50	Joint slot for **Can We Access a Database Both Locally and Privately?** Elette Boyle, Yuval Ishai, Rafael Pass, and Mary Wootters AND **Towards Doubly Efficient Private Information Retrieval** Ran Canetti, Justin Holmgren, and Silas Richelson
13:50-14:10	**Strengthening the Security of Encrypted Databases: Non-Transitive JOINs** Ilya Mironov, Gil Segev, and Ido Shahaf
	Leakage and tampering
14:10-14:30	**How to Construct a Leakage-Resilient (Stateless) Trusted Party** Daniel Genkin, Yuval Ishai, and Mor Weiss
14:30-14:50	**Blockwise p-Tampering Attacks on Cryptographic Primitives, Extractors, and Learners** Saeed Mahloujifar and Mohammad Mahmoody
14:50-15:10	Coffee Break
	Block-Chains

15:10-15:30	**Overcoming Cryptographic Impossibility Results Using Blockchains** Rishab Goyal and Vipul Goyal
	Hardness of Assumptions
15:30-15:50	**On Iterative Collision Search for LPN and Subset Sum** Srinivas Devadas, Ling Ren, and Hanshen Xiao
15:50-16:10	**Can PPAD Hardness be Based on Standard Cryptographic Assumptions?** Alon Rosen, Gil Segev, and Ido Shahaf
16:10-16:30	Break
	Impossibilities and Barriers
16:30-16:50	**Barriers to Black-Box Constructions of Traitor Tracing Systems** Bo Tang and Jiapeng Zhang
16:50-17:10	**On the impossibility of entropy reversal, and its application to zero-knowledge proofs** Shachar Lovett and Jiapeng Zhang
17:10-17:30	**Position-Based Cryptography and Multiparty Communication Complexity** Joshua Brody, Stefan Dziembowski, Sebastian Faust, and Krzysztof Pietrzak

	Tuesday, November 14 (Charles Commons Conference Center)
	Signatures and VRFs
09:00-09:20	Joint slot for **A Generic Approach to Constructing and Proving Verifiable Random Functions** Rishab Goyal, Susan Hohenberger, Venkata Koppula, and Brent Waters AND **Verifiable Random Functions from Non-Interactive Witness-Indistinguishable Proofs** Nir Bitansky
09:20-09:40	**An Equivalence Between Attribute-Based Signatures and Homomorphic Signatures, and New Constructions for Both** Rotem Tsabary
09:40-10:00	**On the One-Per-Message Unforgeability of (EC)DSA and its Variants** Manuel Fersch, Eike Kiltz, and Bertram Poettering
	Fully Homomorphic Encryption
10:00-10:20	**Batched Multi-hop Multi-key FHE from Ring-LWE with Compact Ciphertext Extension** Long Chen, Zhenfeng Zhang, and Xueqing Wang
10:20-10:50	Coffee Break
	Encryption
10:50-11:10	**The Edited Truth** Shafi Goldwasser, Saleet Klein, and Daniel Wichs
11:10-11:30	**A Modular Analysis of the Fujisaki-Okamoto Transformation** Kathrin Hoevelmanns, Dennis Hofheinz, and Eike Kiltz
11:30-11:50	**From Selective IBE to Full IBE and Selective HIBE** Nico Döttling and Sanjam Garg
11:50-12:10	**Multi-Key Authenticated Encryption with Corruptions: Reductions are Lossy** Tibor Jager, Martijn Stam, Ryan Stanley-Oakes, and Bogdan Warinschi
12:10-13:30	Lunch
	Proofs of Work and Space

13:30-13:50	**On the Depth-Robustness and Cumulative Pebbling Cost of Argon2i** Jeremiah Blocki and Samson Zhou
13:50-14:10	**Bandwidth Hard Functions for ASIC Resistance** Ling Ren and Srinivas Devadas
14:10-14:30	**Moderately Hard Functions: Definition, Instantiations, and Applications** Joël Alwen and Björn Tackmann
14:30-14:50	Break
	Secret Sharing
14:50-15:10	**Evolving Secret Sharing: Supporting Dynamic Thresholds and Robustness** Ilan Komargodski and Anat Paskin-Cherniavsky
15:10-15:30	**Linear Secret-Sharing Schemes for Forbidden Graph Access Structures** Amos Beimel, Oriol Farràs, Yuval Mintz, and Naty Peter
15:30-15:50	**Near-Optimal Secret Sharing and Error Correcting Codes in AC0** Kuan Cheng, Yuval Ishai, and Xin Li
15:50-16:10	Coffee Break
	Non-malleable Codes
16:10-16:30	**Inception Makes Non-malleable Codes Stronger** Divesh Aggarwal, Tomasz Kazana, and Maciej Obremski
16:30-16:50	**Four-state Non-malleable Codes with Explicit Constant Rate** Bhavana Kanukurthi, Lakshmibhavana Obbattu, and Sruthi Sekar
	ORAM
16:50-17:10	**Circuit OPRAM: Unifying Statistically and Computationally Secure ORAMs and OPRAMs** T-H. Hubert Chan and Elaine Shi
	Aquarium
17:30-18:30	Transition to the Aquarium
18:30-19:45	Aquarium Tour and Reception
	Invited Talk
19:45-20:45	Chris Peikert and Alon Rosen
	Business Meeting and Rump Session
20:45-22:00	Business Meeting and Rump Session

	Wednesday, November 15 (Charles Commons Conference Center)
	MPC With Few Rounds
09:00-09:20	**On Secure Two-Party Computation in Three Rounds** Prabhanjan Ananth and Abhishek Jain
09:20-09:40	**Four Round Secure Computation without Setup** Zvika Brakerski, Shai Halevi, and Antigoni Polychroniadou
09:40-10:10	Joint slot for **Delayed-Input Non-Malleable Zero Knowledge and Multi-Party Coin Tossing in Four Rounds** Michele Ciampi, Rafail Ostrovsky, Luisa Siniscalchi, and Ivan Visconti AND **Round-Optimal Secure Two-Party Computation from Trapdoor Permutations** Michele Ciampi, Rafail Ostrovsky, Luisa Siniscalchi, and Ivan Visconti

10:10-10:30	**Round Optimal Concurrent MPC via Strong Simulation** Saikrishna Badrinarayanan, Vipul Goyal, Abhishek Jain, Dakshita Khurana, and Amit Sahai
10:30-11:00	Coffee Break
	Invited Talk
11:00-12:00	Theory for Society: Fairness in Classification Cynthia Dwork
12:00-13:20	Lunch
	MPC with Fairness
13:20-13:40	**Secure Two-Party Computation with Fairness -- A Necessary Design Principle** Yehuda Lindell and Tal Rabin
13:40-14:00	**Designing Fully Secure Protocols for Secure Two-Party Computation of Constant-Domain Functions** Vanesa Daza and Nikolaos Makriyannis
	UC Secure MPC
14:00-14:20	**A Unified Approach to Constructing Black-box UC Protocols in Trusted Setup Models** Susumu Kiyoshima, Huijia Lin, and Muthuramakrishnan Venkitasubramaniam
14:20-14:40	Break
	Zero-Knowledge and Nomalleable Protocols
14:40-15:00	**Resettably-Sound Resettable Zero Knowledge in Constant Rounds** Wutichai Chongchitmate, Rafail Ostrovsky, and Ivan Visconti
15:00-15:20	**Round Optimal Concurrent Non-Malleability from Polynomial Hardness** Dakshita Khurana
15:20-15:40	**Zero Knowledge Protocols from Succinct Constraint Detection** Eli Ben-Sasson, Alessandro Chiesa, Michael A. Forbes, Ariel Gabizon, Michael Riabzev, and Nicholas Spooner
15:40-16:00	Coffee Break
	MPC Tools
16:00-16:20	**Actively Secure Garbled Circuits with Constant Communication Overhead in the Plain Model** Carmit Hazay, Yuval Ishai, and Muthuramakrishnan Venkitasubramaniam
16:20-16:40	**Adaptively Indistinguishable Garbled Circuits** Zahra Jafargholi, Alessandra Scafuro, and Daniel Wichs
16:40-17:00	**Resource-efficient OT combiners with active security** Ignacio Cascudo, Ivan Damgård, Oriol Farràs, and Samuel Ranellucci

Venue

Welcome Reception Venue

The welcome reception will be at The Johns Hopkins Club. The reception venue in only a 8 minute walk from the conference hotel.

Click here for walking directions from the conference hotel.

Free parking will be available at the Hopkins Club Lot. Additional paid parking is also available at San Martin Garage.

Conference Venue

The conference venue is the Charles Commons Conference Center, Johns Hopkins University. The conference venue in only a 9 minute walk from the conference hotel.

Click here for walking directions from the conference hotel.

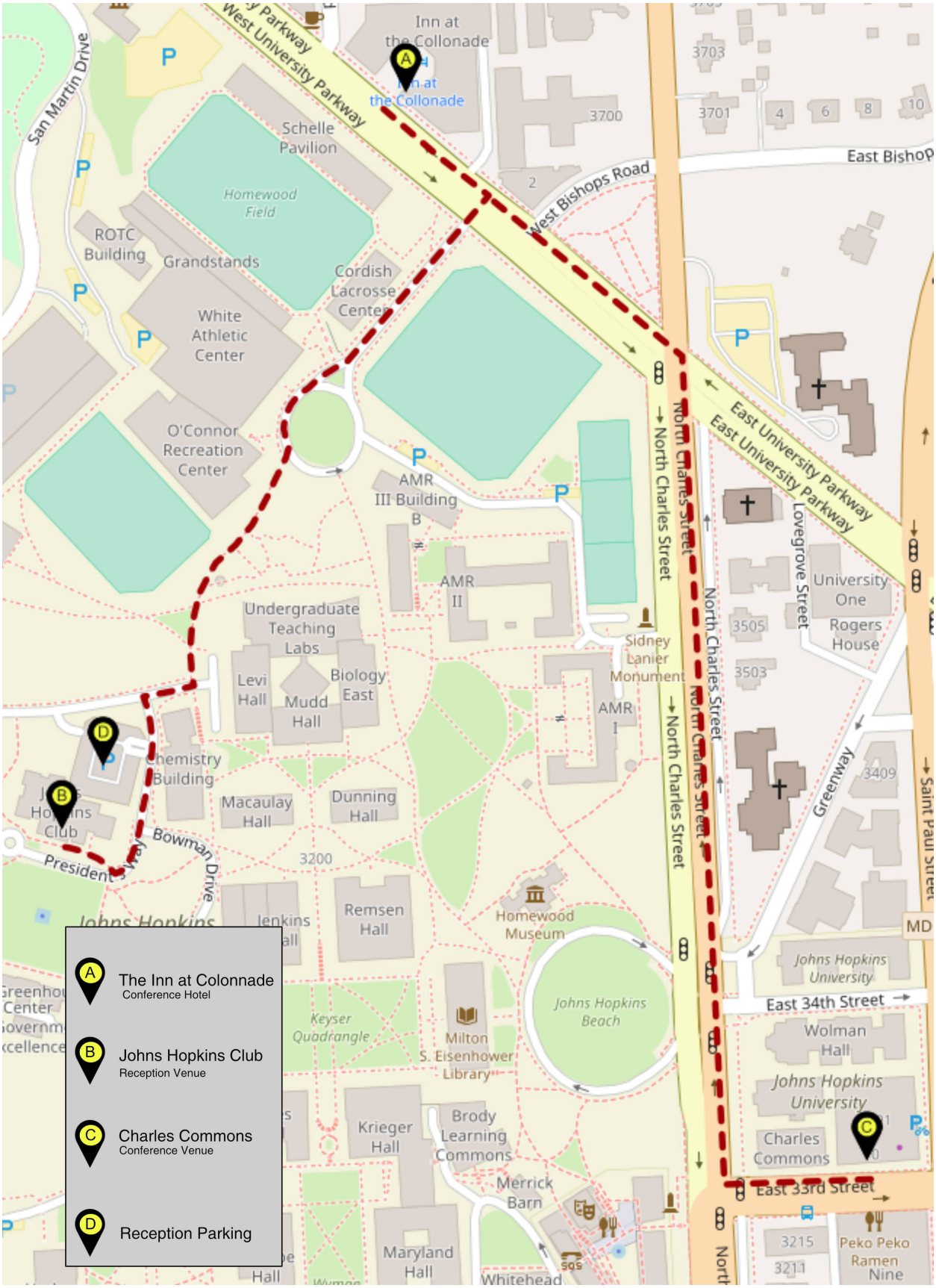
Please use the entrance to the building on the 33rd street.

Parking will be available at 9 E. 33 rd Street, Baltimore, MD 21218.

Tuesday Evening Session Venue

The tuesday evening session will be held at the National Aquarium. Travel to the session venue from the conference venue will be provided.

A map of the locations is provided on the next page.


A
The Inn at Colonnade
Conference Hotel
B
Johns Hopkins Club
Reception Venue
C
Charles Commons
Conference Venue
D
Reception Parking
Inn at the Collonade
San Martin Drive
West University Parkway
Schelle Pavilion
Homewood Field
ROTC Building
Grandstands
Cordish Lacrosse Center
White Athletic Center
O'Connor Recreation Center
AMR III Building B
AMR II
AMR I
Undergraduate Teaching Labs
Levi Hall
Mudd Hall
Biology East
Chemistry Building
Macaulay Hall
Dunning Hall
Bowman Drive
President's Way
Remsen Hall
Homewood Museum
Keyser Quadrangle
Milton S. Eisenhower Library
Johns Hopkins Beach
Krieger Hall
Brody Learning Commons
Merrick Barn
Maryland Hall
Whitehead
Sidney Lanier Monument
North Charles Street
East University Parkway
Lovegrove Street
University One
Rogers House
Greenway
Saint Paul Street
East 34th Street
Wolman Hall
Johns Hopkins University
Charles Commons
East 33rd Street
Peko Peko Ramen Nine
East Bishop
West Bishops Road
3703
3701
3700
3505
3503
3409
3215
3211
3200

Tourist Information

Sight Seeing

The two most prominent art museums in the city are the Baltimore Museum of Art and the Walters Art Museum. Both have impressive collections, and are free for visitors. While the Baltimore Museum of Art is only a 5 minute walk from the conference venue, the Walters Art Museum is more centrally located in Mt. Vernon. A point of note for both museums is that they are closed on Monday and Tuesday.

Of potentially more interest, but a little further away, is the National Cryptographic Museum. It is about 20 miles south-west of the conference venue.

Moving closer to the harbor, the inner harbor has a collection of Historic ships that are within walking distance of each other.

One of Baltimore's most historic monuments is Fort McHenry for its role in the Battle of Baltimore in the early 19th century. The defense of the fort inspired Francis Scott Key to write a poem later to be known as "The Star-Spangled Banner", the national anthem of the USA.

The Baltimore Water Taxi can be an enjoyable ride to explore the various parts of the inner harbor.

For more details on places to visit in Baltimore, you may have a look at the Baltimore Tourism website.

Dining Suggestions

For dining and drinks, some of the more popular (and best) places are around Hampden, Mt. Vernon, Inner Harbor, Federal Hill and Fells point. Baltimore also has an impressive collection of restaurants in Little Italy, located in downtown Baltimore (close to the Harbor). The recommended neighborhoods closest to the conference hotel are Hampden (1 mile) and Mount Vernon (2 miles). The restaurants closest to the conference hotel are located in Roland Park, and are 1-2 blocks away.

Below are a few places that we recommend.

Drinks:

	Type	Location
De Kleine Duivel	Beer	Hampden
Brewer's Art	Beer	Mount Vernon
Power Plant Live	Beer	Inner Harbor
Max's Taphouse	Beer	Fells Point
The Bluebird Cocktail Room	Cocktails	Hampden
Blue pit BBQ and Whiskey Bar	Cocktails	Hampden
Bookmakers Cocktail Club	Cocktails	Federal Hill
Sugarvale	Cocktails	Mount Vernon
Rye	Cocktails	Fells Point
13.5% Wine Bar	Wine	Hampden

Dining:

	Cuisine	Location
Ouzo Bay	Greek Seafood	Inner Harbor
Rusty Scupper	Seafood	Federal Hill
Thames Street Oyster House	Seafood	Fells Point
Azumi	Japanese	Inner Harbor
Joe Benny's	Focaccia Pizza	Little Italy
Puerto 511	Peruvian	Mount Vernon
Mt. Vernon Marketplace	Food Court	Mount Vernon
Blue pit BBQ and Whiskey Bar	BBQ	Hampden
Woodberry Kitchen	New American	Hampden
La Cuchara	Spanish	Hampden
The Food Market	New American	Hampden

	Cuisine	Location
The Arthouse	Gourmet Pizza	Hampden
Paulie Gee	Gourmet Pizza	Hampden
R-House	Food Court	Remington
Cypriana	Mediterranean	Roland Park
Ambassador	Indian	Roland Park