INTERNATIONAL ASSOCIATION FOR CRYPTOLOGIC RESEARCH

iacr

Theory of Cryptography Conference 2019

December 1-5 2019
Nuremberg, Germany

General Chair

Dominique Schröder
University of Erlangen-Nuremberg
Germany

Program Co-Chairs

Alon Rosen
IDC Herzliya
Israel

Dennis Hofheinz
Karlsruhe Institute of Technology
Germany

Department Informatik

ChaAC
Chair of Applied Cryptography

FAU
Friedrich-Alexander Universität Erlangen-Nürnberg

Nuremberg Campus of Technology

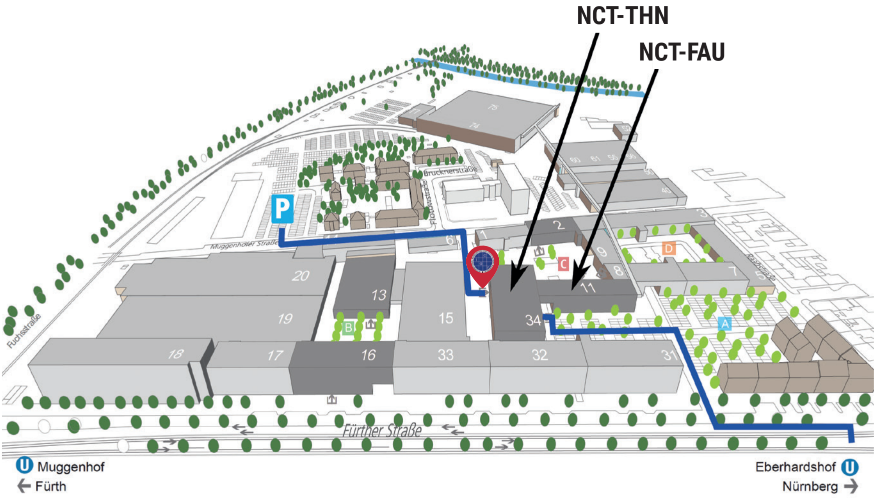
Location for welcome reception and registration, December 1

Chair of Applied Cryptography
Nuremberg Campus of Technology
Fürther Str 246b / house 34 / entrance 7 / 2nd floor
90429 Nürnberg

Arrival by public transport
From Fürth central station take the U1 subway towards Langwasser and exit at Eberhardshof.

From Nuremberg central station take the U1 subway towards Fürth and exit at Eberhardshof.

Arrival by car
Have your navigation find you a way to A73 and exit at Nürnberg/Fürth or Nürnberg Westring.



Location for the main conference, December 2-5

DB Museum Nürnberg
Lessingstraße 6
90443 Nürnberg

Arrival by public transport
From Fürth central station take the S1 towards Hartmannshof, and change at Rothenburger Straße to the U2 towards Flughafen. Exit at Opernhaus.

From Nuremberg central station take the U2 towards Röthenbach and exit at Opernhaus.

Arrival by car
On the motorway, follow the signs for Centrum (city centre) or Hauptbahnhof (main station). Once on the ring road around the historic center, look for Frauentorgraben and then Lessingstraße.

The nearest carparks are located at the city's opera house (Opernhaus: access via Karl-Pschigode-Platz) and Grasersgasse 25 (Sterntor).

WiFi information for DB Museum Nürnberg

DBM WLAN TP8
Password: V038002694976

2019-12-01

18:30 - 20:00

WELCOME RECEPTION AND REGISTRATION

Different location:
Chair of Applied Cryptography
Nuremberg Campus of Technology
Fürther Str 246b / house 34 / entrance 7 / 2nd floor
90429 Nürnberg

2019-12-02

8:00 - 8:45

REGISTRATION

8:45 - 9:00

WELCOME

Joachim Hornegger, President of FAU and
Dominique Schröder, General Chair

9:00 - 10:15

Algebraically Structured LWE, Revisited
Chris Peikert, Zachary Pepin

Lattice Trapdoors and IBE from Middle-Product LWE
Alex Lombardi, Vinod Vaikuntanathan, Thuy Duong {Vuong}

Matrix PRFs: Constructions, Attacks, and Applications to Obfuscation
Yilei Chen, Minki Hhan, Vinod Vaikuntanathan, Hoeteck Wee

10:15 - 10:45

COFFEE BREAK

10:45 - 12:00

Obfuscated Fuzzy Hamming Distance and Conjunctions from Subset Product Problems
Steven D. Galbraith, Lukas Zobernig

A Black-Box Construction of Fully-Simulatable, Round-Optimal Oblivious Transfer from Strongly Uniform Key Agreement
Daniele Friolo, Daniel Masny, Daniele Venturi

Synchronous Consensus with Optimal Asynchronous Fallback Guarantees
Erica Blum, Jonathan Katz, Julian Loss

2019-12-02

12:00 - 13:30

LUNCH

13:30 - 14:45

Predicate Encryption from Bilinear Maps and One-Sided Probabilistic Rank
Josh Alman, Robin Hui

Optimal Bounded-Collusion Secure Functional Encryption
Prabhanjan Ananth, Vinod Vaikuntanathan

From FE Combiners to Secure MPC and Back
Prabhanjan Ananth, Saikrishna Badrinarayanan, Aayush Jain, Nathan Manohar, Amit Sahai

14:45 - 15:15

COFFEE BREAK

15:15 - 16:30

(Pseudo) Random Quantum States with Binary Phase
Zvika Brakerski, Omri Shmueli

General Linear Group Action on Tensors: A Candidate for Post-Quantum Cryptography
Zhengfeng Ji, Youming Qiao, Fang Song, Aaram Yun

Composable and Finite Computational Security of Quantum Message Transmission
Fabio Banfi, Ueli Maurer, Christopher Portmann, Jiamin Zhu

16:30 - 17:00

COFFEE BREAK

17:00 - 18:00

INVITED TALK
A Complexity-Theoretic Perspective on Algorithmic Fairness
Omer Reingold

2019-12-03

9:00 - 10:15

On Fully Secure MPC with Solitary Output
Shai Halevi, Yuval Ishai, Eyal Kushilevitz, Nikolaos Makriyannis, Tal Rabin

Secure Computation with Preprocessing via Function Secret Sharing
Elette Boyle, Niv Gilboa, Yuval Ishai

Efficient Private PEZ Protocols for Symmetric Functions
Yoshiki Abe, Mitsugu Iwamoto, Kazuo Ohta

10:15 - 10:45

COFFEE BREAK

10:45 - 11:10

BEST YOUNG RESEARCHER AWARD
The Function-Inversion Problem: Barriers and Opportunities
Henry Corrigan-Gibbs, Dmitry Kogan

11:10 - 12:00

On the Complexity of Collision Resistant Hash Functions: New and Old Black-Box Separations
Nir Bitansky, Akshay Degwekar

Characterizing Collision and Second-Preimage Resistance in Linicrypt
Ian McQuoid, Mike Rosulek, Trevor Swope

12:00 - 13:30

LUNCH

13:30 - 15:10

Efficient Information-Theoretic Secure Multiparty Computation over Z/p^k Z via Galois Rings
Mark Abspoel, Ronald Cramer, Ivan Damgård, Daniel Escudero, Chen Yuan

Is Information-Theoretic Topology-Hiding Computation Possible?
Marshall Ball, Elette Boyle, Ran Cohen, Tal Malkin, Tal Moran

⋮

2019-12-03

⋮

Channels of Small Log-Ratio Leakage and Characterization of Two-Party Differentially Private Computation
Iftach Haitner, Noam Mazo, Ronen Shaltiel, Jad Silbak

On Perfectly Secure 2PC in the OT-Hybrid Model
Bar Alon, Anat Paskin-Cherniavsky

15:10 - 15:40

COFFEE BREAK

15:40 - 16:55

Succinct Arguments in the Quantum Random Oracle Model
Alessandro Chiesa, Peter Manohar, Nicholas Spooner

Delegating Quantum Computation in the Quantum Random Oracle Model
Jiayu Zhang

Tighter proofs of CCA security in the quantum random oracle model
Nina Bindel, Mike Hamburg, Kathrin Hövelmanns, Andreas Hülsing, Edoardo Persichetti

17:15 - 19:00

BUSINESS MEETING AND RUMP SESSION

19:30 - 22:00

BANQUET DINNER

2019-12-04

9:00 - 10:00

INVITED TALK

Indistinguishability Obfuscation without Multilinear Maps
Rachel Lin

10:00 - 10:30

COFFEE BREAK

10:30 - 12:10

Attribute Based Encryption for Deterministic Finite Automata from DLIN
Shweta Agrawal, Monosij Maitra, Shota Yamada

CPA-to-CCA Transformation for KDM Security
Fuyuki Kitagawa, Takahiro Matsuda

New Approaches to Traitor Tracing with Embedded Identities
Rishab Goyal, Venkata Koppula, Brent Waters

A Unified and Composable Take on Ratcheting
Daniel Jost, Ueli Maurer, Marta Mularczyk

12:10 - 13:45

LUNCH

13:45 - 15:25

Continuously Non-Malleable Secret Sharing for General Access Structures
Gianluca Brian, Antonio Faonio, Daniele Venturi

Interactive Non-Malleable Codes
Nils Fleischhacker, Vipul Goyal, Abhishek Jain, Anat Paskin-Cherniavsky, Slava Radune

Stronger Lower Bounds for Online ORAM
Pavel Hubacek, Michal Koucky, Karel Kral, Veronika Slivova

Adaptively Secure Garbling Schemes for Parallel Computations
Kai-Min Chung, Luowen Qian

16:00 - 22:00

EXCURSION

2019-12-05

9:00 - 10:00

TCC TEST OF TIME AWARD TALK

How bad is worst-case data if you know where it comes from?
Paul Valiant

10:00 - 10:30

COFFEE BREAK

10:30 - 12:10

Statistical Difference Beyond the Polarizing Regime
Itay Berman, Akshay Degwekar, Ron D. Rothblum, Prashant Nalini Vasudevan

Estimating Gaps in Martingales and Applications to Coin-Tossing: Constructions & Hardness
Hamidreza Amini Khorasgani, Hemanta K. Maji, Tamalika Mukherjee

Fully Homomorphic NIZK and NIWI Proofs
Prabhanjan Ananth, Apoorvaa Deshpande, Yael Tauman Kalai, Anna Lysyanskaya

Lower and Upper Bounds on the Randomness Complexity of Private Computations of AND
Eyal Kushilevitz, Rafail Ostrovsky, Emmanuel Prouff, Adi Rosén, Adrian Thillard, Damien Vergnaud

12:10 - 13:45

LUNCH

13:45 - 15:00

Leveraging Linear Decryption: Rate-1 Fully-Homomorphic Encryption and Time-Lock Puzzles
Zvika Brakerski, Nico Döttling, Sanjam Garg, Giulio Malavolta

Compressible FHE with Applications to PIR
Craig Gentry, Shai Halevi

Permuted Puzzles and Cryptographic Hardness
Elette Boyle, Justin Holmgren, Mor Weiss

15:00 - 15:30

COFFEE BREAK

15:30 - 16:45

Linear-Size Constant-Query IOPs for Delegating Computation
Eli Ben-Sasson, Alessandro Chiesa, Lior Goldberg, Tom Gur, Michael Riabzev, Nicholas Spooner

On the (In)security of Kilian-Based SNARGs
James Bartusek, Liron Bronfman, Justin Holmgren, Fermi Ma, Ron D. Rothblum

Incrementally Verifiable Computation via Incremental PCPs
Moni Naor, Omer Paneth, Guy N. Rothblum

Special Thanks to our Sponsors: