TCC 2016-B

14th IACR Theory of Cryptography Conference

(http://tcc2016b.sklois.cn/)

Handbook

October 31 - November 3, 2016
Beijing Friendship Hotel, China

Honorary Chair:

Andrew Chi-Chih Yao (IIIS, Tsinghua University, China)

General Chair:

Dongdai Lin (SKLOIS, Institute of Information Engineering, CAS, China)

Program Committee Co-Chairs:

Martin Hirt (ETH Zurich)

Adam Smith (Penn State)

Organizing Committee:

Kefei Chen (Hangzhou Normal University, China)

Yi Deng (SKLOIS, Institute of Information Engineering, CAS, China)

Shuqin Fan (State Key Laboratory of Cryptology, China)

Lei Hu (SKLOIS, Institute of Information Engineering, CAS, China)

Xinyi Huang (Fujian Normal University, China)

Hui Li (Xidian University, China)

Xiaoming Sun (Institute of Computing Technology, CAS, China)

Xiaoyun Wang (Tsinghua University, China)

Jian Weng (Jinan University, China)

Yu Yu (Shanghai Jiao Tong University, China)

Fangguo Zhang (Sun Yat-sen University, China)

Program Sketch

14th IACR Theory of Cryptography Conference (TCC 2016-B)
October 31 - November 3, 2016, Beijing China

Oct. 31	14:00-18:00	Conference on site registration	Lobby of Building No. 4
	18:00-20:00	Reception	Friendship Palace
Nov. 1	8:00-9:00	Conference on site registration	Meeting Room 1 Building No. 7
	9:00-10:00	Conference Talks	
	10:00-10:30	Break	
	10:30-12:45	Conference Talks	
	12:45-14:00	Lunch	Friendship Palace
	14:00-15:00	Conference Talks	Meeting Room 1 Building No. 7
	15:00-15:30	Break	
	15:30-17:10	Conference Talks	
	18:00-20:30	Conference Banquet	Friendship Palace
Nov. 2	9:00-10:05	Conference Talks	Meeting Room 1 Building No. 7
	10:05-10:35	Break	
	10:35-12:35	Conference Talks	
	12:35-14:00	Lunch	Friendship Palace
	14:00-15:20	Conference Talks	Meeting Room 1 Building No. 7
	15:20-15:50	Break	
	15:50-17:10	Conference Talks	
	17:30-19:00	Dinner	Friendship Palace
	19:00-19:30	Business Meeting	Meeting Room 1 Building No. 7
	19:30-21:30	Rump Session	
Nov. 3	9:00-10:25	Conference Talks	Meeting Room 1 Building No. 7
	10:25-10:55	Break	
	10:55-12:35	Conference Talks	
	12:35-14:00	Lunch	Friendship Palace
	14:00-15:00	Conference Talks	Meeting Room 1 Building No. 7
	15:00-15:30	Break	
	15:30-17:15	Conference Talks	
	17:15-	Farewell with tears	Anywhere
Nov. 4	Tour guide by a tourist agency, cost on your own, subject to individual interests.		

TCC 2016-B Tentative Program

MONDAY Building 4, Lobby

14:00-18:00 Conference on-site registrations

18:00-20:00 Reception

TUESDAY Building 7, Room 1

8:00-9:00 Conference on-site registrations

Foundations I (Chair: John Steinberger)

9:00-9:20
Simulating Auxiliary Inputs, Revisited
Maciej Skorski

9:20-9:40
Fast Pseudorandom Functions Based on Expander Graphs
Benny Applebaum, Pavel Raykov

9:40-10:00
3-Message Zero Knowledge Against Human Ignorance
Nir Bitansky, Zvika Brakerski, Yael Kalai, Omer Paneth, Vinod Vaikuntanathan

10:00-10:30 BREAK

Unconditional Security I (Chair: Andrej Bogdanov)

10:30-10:50
Pseudoentropy: Lower-bounds for Chain rules and Transformations
Krzysztof Pietrzak, Maciej Skorski

10:50-11:10
Oblivious Transfer from Any Non-Trivial Elastic Noisy Channel via Secret Key Agreement
Ignacio Cascudo, Ivan Damgård, Felipe Lacerda, Samuel Ranellucci

11:10-11:30
Simultaneous Secrecy and Reliability Amplification for a General Channel Model
Russell Impagliazzo, Ragesh Jaiswal, Valentine Kabanets, Bruce M. Kapron, Valerie King, Stefano Tessaro

Test of Time Award (Chair: Adam Smith)

11:30-12:45
From Indifferentiability to Constructive Cryptography (and Back)
Ueli Maurer, Renato Renner

12:45-14:00 LUNCH Friendship Palace

Foundations II (Chair: Alessandro Chiesa)

14:00-14:20
On the (In)security of SNARKs in the Presence of Oracles
Dario Fiore, Anca Nitulescu

14:20-14:40
Leakage Resilient One-Way Functions: The Auxiliary-Input Setting
Ilan Komargodski

14:40-15:00
The GGM Function Family is Weakly One-Way
Aloni Cohen, Saleet Klein

15:00-15:30 BREAK

Foundations of Multi-Party Protocol (Chair: Alon Rosen)

15:30-15:50
Almost-Optimally Fair Multiparty Coin-Tossing with Nearly Three-Quarters Malicious
Bar Alon, Eran Omri

15:50-16:10
Binary AMD Circuits from Secure Multiparty Computation
Daniel Genkin, Yuval Ishai, *Mor Weiss*

16:10-16:30
Composable Security in the Tamper-Proof Hardware Model under Minimal Complexity
Carmit Hazay, Antigoni Polychroniadou, Muthuramakrishnan Venkitasubramaniam

16:30-16:50
Composable Adaptive Secure Protocols without Setup under Polytime Assumptions
Carmit Hazay, Muthuramakrishnan Venkitasubramaniam

16:50-17:10
Adaptive Security of Yao's Garbled Circuits
Zahra Jafargholi, Daniel Wichs

18:00-20:30 Conference Banquet Friendship Palace

WEDNESDAY Building 7, Room 1

Delegation and IP (Chair: Muthuramakrishnan Venkitasubramaniam)

9:00-9:25
Delegating RAM Computations with Adaptive Soundness and Privacy
Prabhanjan Ananth, Yu-Chi Chen, Kai-Min Chung, Huijia Lin, Wei-Kai Lin

JOINT SLOT WITH

Adaptive Succinct Garbled RAM, or How To Delegate Your Database
Ran Canetti, Yilei Chen, Justin Holmgren, Mariana Raykova

9:25-9:45
Interactive Oracle Proofs
Eli Ben-Sasson, Alessandro Chiesa, Nicholas Spooner

9:45-10:05
Delegating RAM Computations
Yael Kalai, Omer Paneth

10:05-10:35 BREAK

Differential Privacy (Chair: Martin Hirt)

10:35-10:55
Separating Computational and Statistical Differential Privacy in the Client-Server Model
Mark Bun, Yi-Hsiu Chen, Salil P. Vadhan

10:55-11:15
Concentrated Differential Privacy: Simplifications, Extensions, and Lower Bounds
Mark Bun, Thomas Steinke

11:15-11:35
Strong Hardness of Privacy from Weak Traitor Tracing
Lucas Kowalczyk, Tal Malkin, Jonathan Ullman, Mark Zhandry

Invited Talk (Chair: Martin Hirt)

11:35-12:35
Through the Looking Glass: What Cryptography Should Do for Alice
Allison Bishop

12:35-14:00 LUNCH Friendship Palace

Public-Key Encryption I (Chair: Andrej Bogdanov)

14:00-14:20
Towards Non-Black-Box Separations of Public Key Encryption and One Way Function
Dana Dachman-Soled

14:20-14:40
Post-Quantum Security of the Fujisaki-Okamoto and OAEP Transforms
Ehsan Ebrahimi Targhi, Dominique Unruh

Secret Sharing (Chair: Andrej Bogdanov)

14:40-15:00
Threshold Secret Sharing Requires a Linear Size Alphabet
Andrej Bogdanov, Siyao Guo, Ilan Komargodski

15:00-15:20
How to Share a Secret, Infinitely
Ilan Komargodski, Moni Naor, Eylon Yogev

15:20-15:50 BREAK

New Models (Chair: Alon Rosen)

15:50-16:10
Designing Proof of Human-work Puzzles for Cryptocurrency and Beyond
Jeremiah Blocki, Hong-Sheng Zhou

16:10-16:30
Access Control Encryption: Enforcing Information Flow with Cryptography
Ivan Damgård, *Helene Haagh*, Claudio Orlandi

Obfuscation and Multilinear Maps (Chair: Alon Rosen)

16:30-16:50
Secure Obfuscation in a Weak Multilinear Map Model
Sanjam Garg, Eric Miles, Pratyay Mukherjee, Amit Sahai, Akshayaram Srinivasan, Mark Zhandry

16:50-17:10
Virtual Grey-Boxes Beyond Obfuscation: A Statistical Security Notion for Cryptographic Agents
Shashank Agrawal, Manoj Prabhakaran, Ching-Hua Yu

19:00-19:30 Business Meeting

19:30-21:30 Rump Session

THURSDAY Building 7, Room 1

Round Complexity & Efficiency of Multi-Party Computation (Chair: Alessandro Chiesa)

9:00-9:20
Efficient Secure Multiparty Computation with Identifiable Abort
Carsten Baum, Emmanuela Orsini, *Peter Scholl*

9:20-9:45
Secure Multiparty RAM Computation in Constant Rounds
Sanjam Garg, Divya Gupta, *Peihan Miao*, Omkant Pandey

JOINT SLOT WITH

Constant-Round Maliciously Secure Two-Party Computation in the RAM Model
Carmit Hazay, *Avishay Yanai*

9:45-10:05
More Efficient Constant-Round Multi-Party Computation from BMR and SHE
Yehuda Lindell, Nigel P. Smart, *Eduardo Soria-Vazquez*

10:05-10:25
Cross&Clean: Amortized Garbled Circuits With Constant Overhead
Jesper Buus Nielsen, Claudio Orlandi

10:25-10:55 BREAK

Unconditional Security II (Chair: Adam Smith)

10:55-11:15
Proof of Space from Stacked Expanders
Ling Ren, Srinivas Devadas

11:15-11:35
Perfectly Secure Message Transmission in Two Rounds
Gabriele Spini, Gilles Zémor

Invited Talk (Chair: Adam Smith)

11:35-12:35
Secure Hardware and Cryptography: Contrasts, Challenges and Opportunities
Srini Devadas

12:35-14:00 LUNCH Friendship Palace

Public-Key Encryption II (Chair: Muthuramakrishnan Venkitasubramaniam)

14:00-14:20
Standard Security Does Not Imply Indistinguishability Under Selective Opening
Dennis Hofheinz, Vanishree Rao, Daniel Wichs

14:20-14:40
Public-Key Encryption with Simulation-Based Selective-Opening Security and

Compact Ciphertexts
Dennis Hofheinz, Tibor Jager, Andy Rupp

14:40-15:00
Multi-Key FHE from LWE, Revisited
Chris Peikert, Sina Shiehian

15:00-15:30 BREAK

Attribute-Based Encryption (Chair: John Steinberger)

15:30-15:50
Deniable Attribute Based Encryption for Branching Programs from LWE
Daniel Apon, *Xiong Fan*, Feng-Hao Liu

15:50-16:10
Targeted Homomorphic Attribute-Based Encryption
Zvika Brakerski, David Cash, *Rotem Tsabary*, Hoeteck Wee

16:10-16:30
Semi-Adaptive Security and Bundling Functionalities Made Generic and Easy
Rishab Goyal, Venkata Koppula, Brent Waters

Functional Encryption (Chair: John Steinberger)

16:30-16:50
From Cryptomania to Obfustopia through Secret-Key Functional Encryption
Nir Bitansky, Ryo Nishimaki, Alain Passelègue, Daniel Wichs

16:50-17:15
Single-Key to Multi-Key Functional Encryption with Polynomial Loss
Sanjam Garg, Akshayaram Srinivasan

JOINT SLOT WITH

Compactness vs Collusion Resistance in Functional Encryption
Baiyu Li, Daniele Micciancio

17:15 FAREWELL

Introduction to

State Key Laboratory of Information Security

The State Key Laboratory of Information Security (SKLOIS) was first formed in 1989, and was officially established and opened to the public in 1991. The laboratory is administered by the Chinese Academy of Sciences (CAS). Since 2012, the laboratory has been affiliated to the Institute of Information Engineering of CAS.

The SKLOIS commits itself as to providing a scientific foundation for information security, doing research in information security theory, developing critical technology, and cultivating high-level specialists in information security.

Since its establishment, the SKLOIS has made great achievements in information security theory and technology. By December 2015, SKLOIS published more than 3,500 papers and 110 books, owned 96 patents and 326 software copyrights, and drafted 40 domestic standards and 4 international standards. The laboratory has completed more than 660 important projects, including National Key Foundation Theory Research and Natural Science Foundation projects, and received 31 awards from the Central Government or National Ministries. The awards include one first prize and 5 second prizes of State Scientific and Technological Progress Awards, 2 third prizes of State Natural Science Awards, and 14 first prizes of National Ministry Awards. As of December 2015, the SKLOIS has 205 permanent staff members and 400 temporary members. The SKLOIS has 8800 square meters office area, and has first-class experimental facilities in China for information security research.

Conference Information

Conference Venue: Meeting Room No. 1 of Building No. 7

Beijing Friendship Hotel (北京友谊宾馆，瑞宾楼1号会议室)

Registration Information

October 31,	14:00-18:00.	Lobby of Building No. 4
November 1-2,	08:30-18:00.	Lobby of Building No. 7 (Conference site)
November 3,	08:30-12:00.	Lobby of Building No. 7 (Conference site)

Lunches and dinners: Tickets for registered participants are in the registration bags. Lunches and dinners are served inside the Friendship Palace, specific location needs to follow the instructions.

Taxi: Taxies can be found at the front gate of Building NO. 4. You may ask the hotel front desk to make a booking.

Contact information:

Ms Qi Dai, 15120086798 (cell), Professor Yi Deng, 18610995467 (cell)

Conference webpage: http://tcc2016b.sklois.cn/

Transportation from Airport:

Airport Shuttle Bus: Take *Gong Zhu Fen* Line and get off at *Friendship Hotel Station*;

Subway: *Airport express* —*Line 10* —*Line 4* and get off at *Renmin Univ. Station;*

Taxi: It is about 35 km, takes one hour and cost about 120 CNY up to traffic and time.