PKC 2019

22nd International Conference on Theory and Practice in Public Key Cryptography

Preliminary Program

April 14-17, 2019
Beijing, China

Program Sketch

22nd International Conference on Practice and Theory of Public Key Cryptography

(PKC 2019)

April 14–17, 2019, Beijing China

April 14	16:00-18:00	Conference on site registration	
	18:00-21:00	Reception	
April 15	8:00-9:00	Conference on site registration	
	9:00-9:20	Opening Remarks	
	9:20-10:20	Invited Talk	
	10:20-10:40	Group Photo	
	11:00-12:15	Session 1	
	12:20-13:30	Lunch	
	13:30-15:35	Session 2	
	16:00-18:05	Session 3	
	18:30-19:30	Dinner	
April 16	9:00-10:40	Session 4	
	11:00-12:15	Session 5	
	12:20-13:30	Lunch	
	13:30-14:30	Test of Time Award Ceremony	
	14:30-15:45	Session 6	
	16:15-17:55	Session 7	
	18:30-21:00	Conference Banquet	
April 17	9:00-10:40	Session 8	
	11:00-12:15	Session 9	
	12:20-13:30	Lunch	
	13:30-15:10	Session 10	
	15:40-17:20	Session 11	
April 18	Tour guide by a tourist agent, cost on your own, subject to individual interests.		

Note: All presentations are in Functional Hall in Building No.1 (贵宾楼多功能厅)

Advanced Program

22nd International Conference on Practice and Theory of Public Key Cryptography

(PKC 2019)

Beijing Friendship Hotel

April 14, 2019	
16:00-18:00	**Conference on site registration**
18:00-21:00	**Reception**
April 15, 2019	
8:00-9:00	**Conference on site registration**
9:00-9:20	**Opening Remarks**
Invited Talk **Session Chair:**	
9:20-10:20	**TBA** *Tatsuaki Okamoto*
10:20-10:40	**Group photo**
10:40-11:00	**Coffee Break**
Session 1: Cryptographic Protocols **Session Chair:**	
11:00-11:25	180. Sub-logarithmic Distributed Oblivious RAM with Small Block Size
	Eyal Kushilevitz; Tamer Mour
11:25-11:50	156. Lossy Algebraic Filters With Short Tags
	Benoît Libert; Chen Qian
11:50-12:15	247. Non-Interactive Keyed-Verification Anonymous Credentials
	Geoffroy Couteau; Michael Reichle
12:20-13:30	**Lunch**
Session 2: Digital Signatures **Session Chair:**	
13:30-13:55	142. Shorter Ring Signatures from Standard Assumptions
	Alonso Gonzalez
13:55-14:20	168. Efficient Attribute-Based Signatures for Unbounded Arithmetic Branching Programs
	Pratish Datta; Tatsuaki Okamoto; Katsuyuki Takashima
14:20-14:45	217. Efficient Invisible and Unlinkable Sanitizable Signatures
	Xavier Bultel; Pascal Lafourcade; Russell W. F. Lai; Giulio Malavolta; Dominique Schröder; Sri Aravinda Krishnan Thyagarajan
14:45-15:10	256. Group Signatures with Selective Linkability
	Lydia Garms and Anja Lehmann
15:10-15:35	263. Let a Non-Barking Watchdog Bite: Cliptographic Signatures with an Offline Watchdog
	Sherman S. M. Chow; Alexander Russell; Qiang Tang; Moti Yung; Yongjun Zhao;

	Hong-Sheng Zhou
15:35-16:00	**Coffee Break**
Session 3: Zero-Knowledge **Session Chair:**	
16:00-16:25	255. Zero-Knowledge Elementary Databases with More Expressive Queries
	Benoît Libert; Khoa Nguyen; Benjamin Hong Meng Tan; Huaxiong Wang
16:25-16:50	272. Efficient Non-Interactive Zero-Knowledge Proofs in Cross-Domains without Trusted Setup
	Michael Backes; Lucjan Hanzlik;Amir Herzberg; Aniket Kate; Ivan Pryvalov
16:50-17:15	252. Shorter Quadratic QA-NIZK Proofs
	Vanesa Daza;Alonso González;Zaira Pindado;Carla Ràfols;Javier Silva
17:15-17:40	236. Short Discrete Log Proofs for FHE and Ring-LWE Ciphertexts
	Rafael del Pino; Vadim Lyubashevsky; Gregor Seiler
17:40-18:05	270. Publicly Verifiable Proofs from Blockchains
	Alessandra Scafuro;Luisa Siniscalchi;Ivan Visconti
18:30-19:30	**Dinner**
April 16, 2019	
Session 4: **Identity-Based Encryption** **Session Chair:**	
9:00-9:25	190. Identity-based Broadcast Encryption with Efficient Revocation
	Aijun Ge; Puwen Wei
9:25-9:50	254.Tightly secure hierarchical identity-based encryption
	Roman Langrehr; Jiaxin Pan
9:50-10:15	150. Leakage-resilient Identity-based Encryption in Bounded Retrieval Model with Nearly Optimal Leakage-Ratio
	Ryo Nishimaki;Takashi Yamakawa
10:15-10:40	239.Additively Homomorphic IBE from eth Residuosity
	Michael Clear; Ciaran McGoldrick
10:40-11:00	**Coffee Break**
Session 5: Fundamental Primitives (I) **Session Chair:**	
11:00-11:25	224. Upper and Lower Bounds for Continuous Non-Malleable Codes
	Dana Dachman-Soled; Mukul Kulkarni
11:25-11:50	273. Improved Security Evaluation Techniques for Imperfect Randomness from Arbitrary Distributions
	Takahiro Matsuda; Kenta Takahashi; Takao Murakami; Goichiro Hanaoka
11:50-12:15	105. On Tightly Secure Primitives in the Multi-Instance Setting
	Dennis Hofheinz; Ngoc Khanh Nguyen
12:20-13:30	**Lunch**
Test of Time Award **Session Chair:**	
13:30-14:30	Ceremony & Talk
Session 6: Public Key Encryptions **Session Chair:**	

14:30-14:55	110. Collusion Resistant Broadcast and Trace from Positional Witness Encryption
	Rishab Goyal; Satyanarayana Vusirikala; Brent Waters
14:55-15:20	235. Break-glass Encryption
	Alessandra Scafuro
15:20-15:45	244. Registration-Based Encryption from Standard Assumptions
	Sanjam Garg; Mohammad Hajiabadi; Mohammad Mahmoody; Ahmadreza Rahimi; Sruthi Sekar
15:45-16:15	**Coffee Break**
Session 7: Functional Encryption **Session Chair:**	
16:15-16:40	123. FE for Inner Products and Its Application to Decentralized ABE
	Zhedong Wang; Xiong Fan; Feng-Hao Liu
16:40-17:05	242. Decentralizing Inner-Product Functional Encryption
	Michel Abdalla; Fabrice Benhamouda; Markulf Kohlweiss; Hendrik Waldner
17:05-17:30	128. Non-Zero Inner Product Encryption Schemes from Various Assumptions: LWE, DDH and DCR
	Shuichi Katsumata; Shota Yamada
17:30-17:55	175. Function Private Predicate Encryption for Low Min-Entropy Predicates
	Sikhar Patranabis; Debdeep Mukhopadhyay; Somindu C. Ramanna
18:30-21:00	**Banquet**
April 17, 2019	
Session 8: **Obfuscation based Cryptography & Re-encryption Schemes** **Session Chair:**	
9:00-9:25	159. Adaptively Single-key Secure Constrained PRFs for NC1
	Nuttapong Attrapadung;Takahiro Matsuda; Ryo Nishimaki; Shota Yamada; Takashi Yamakawa
9:25-9:50	260. Obfuscating simple functionalities from knowledge assumptions
	Ward Beullens; Hoeteck Wee
9:50-10:15	201. Adaptively Secure Proxy Re-encryption
	Georg Fuchsbauer; Chethan Kamath; Karen Klein; Krzysztof Pietrzak
10:15-10:40	232. What about Bob? The Inadequacy of CPA Security for Proxy Reencryption
	Aloni Cohen
10:40-11:00	**Coffee Break**
Session 9: Fundamental Primitives (II) **Session Chair:**	
11:00-11:25	129. General Constructions of Robustly Reusable Fuzzy Extractor
	Yunhua Wen; Shengli Liu; Dawu Gu
11:25-11:50	140. Safety in Numbers: On the Need for Robust Diffie-Hellman Parameter Validation
	Steven D. Galbraith; Jake Massimo; Kenneth G. Paterson
11:50-12:15	202. Hunting and Gathering - Verifiable Random Functions from Standard Assumptions with Short Proofs
	Lisa Kohl
12:20-13:30	**Lunch**
Session 10: Post Quantum Cryptography (I)	

Session Chair:	
13:30-13:55	163. Lattice-based Revocable (Hierarchical) IBE with Decryption Key Exposure Resistance
	Shuichi Katsumata; Takahiro Matsuda; Atsushi Takayasu
13:55-14:20	238. Towards Non-Interactive Zero-Knowledge for NP from LWE
	Ron D. Rothblum; Adam Sealfon; Katerina Sotiraki
14:20-14:45	276. More Efficient Algorithms for the NTRU Key Generation using the Field Norm
	Thomas Pornin; Thomas Prest
14:45-15:10	216. Efficiently Masking Binomial Sampling at Arbitrary Orders for Lattice Based Crypto
	Tobias Schneider; Clara Paglialonga; Tobias Oder; Tim Güneysu
15:10-15:40	**Coffee Break**
Session 11: Post Quantum Cryptography (II) **Session Chair:**	
15:40-16:05	193. Decryption Failure Attacks on IND-CCA Secure Lattice-Based Schemes
	Jan-Pieter D'Anvers; Qian Guo; Thomas Johansson; Alexander Nilsson; Frederik Vercauteren; Ingrid Verbauwhede
16:05-16:30	172. Key Encapsulation Mechanism with Explicit Rejection in the Quantum Random Oracle Model
	Haodong Jiang; Zhenfeng Zhang; Zhi Ma
16:30-16:55	109. Reducing the Key Size of McEliece Cryptosystem from Automorphisminduced Goppa Codes via Permutations
	Zhe Li; Chaoping Xing; Sze Ling Yeo
16:55-17:20	121. On the (non) obfuscating power of Garside Normal Forms
	Simon-Philipp Merz; Christophe Petit
17:20-	**Farewell with Tears (anywhere)**
April 18, 2019	
Tour guide by local travel agent (subject to your own interest)	

Conference Information

Conference Venue: Functional Hall of Building No. 1

Beijing Friendship Hotel (北京友谊宾馆，贵宾楼多功能厅)

Registration Information

April 14, 14:00-18:00. Lobby of Building No. 1
April 15-16, 08:30-18:00. Lobby of Building No. 1 (Conference site)
April 17, 08:30-12:00. Lobby of Building No. 1 (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 gates of Building NO. 2 and Grand Building. You may ask the hotel front desk to make a booking.

Contact information:

Professor Baofeng Wu: 134 2607 6355(cell), Dr. Anyu Wang: 15201173389(cell)

Conference webpage: http://pkc.iarc.org/2019/

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 150 CNY up to traffic and time.