Sponsors

Gold level — ANT RESEARCH — National Financial Cryptography Research Center

Silver level — sansec 三未信安 — 天融信 TOPSEC

Bronze level — IBM — Meta — SANGFOR 深信服科技

Asiacrypt 2023

Conference Program

The 29th International Conference on the
Theory and Application of Cryptology
and Information Security

December 4-8, 2023, Guangzhou, China

International Association for Cryptologic Research — 暨南大學 JINAN UNIVERSITY — 中山大學 SUN YAT-SEN UNIVERSITY

AGENDA

WELCOME MESSAGE

On behalf of the local organizing committee, Jinan University and Sun Yat-sen University, we are delighted to welcome you to Guangzhou.

Asiacrypt 2023 will be held December 4-8 2023 with an excellent program consisting of two prestigious keynote speakers, 106 compelling paper presentations, and the traditional rump session. This handbook gives you the detailed schedule of the program.

Apart from attending this one of the flagship conferences in cryptography, we do wish that you will have a chance to explore our wonderful city in your spare time.

Finally, we would like to take this opportunity to thank the many people who have contributed to Asiacrypt 2023. Special thanks go to every member of the local organizing team and our gracious sponsors (ANT Research, National Financial Cryptography Research Center, SANSEC, TOPSEC, IBM, Meta, SANGFOR). We hope you thoroughly enjoy the conference.

Jian Weng

Fangguo Zhang

Asiacrypt 2023 General Co-chairs

ORGANIZERS

SPONSORS

We thank all our sponsors for their support.

HIGHLIGHTS OF GUANGZHOU FACTS

Climate
Average highest temperature in July: 32.8 °C (90.9 °F)

Average lowest temperature in January: 10.3 °C (50.5 °F)

Humid subtropical climate with annual monsoons from April to September; annual precipitation: 1,735 mm (68.3 in). There is a sudden onset of the monsoon season involving rainfall and a change of temperature each spring.

Economy
Development: Developed, the per capita income is among the highest of China's large cities. It is an electronics and clothing manufacture center and a trade hub for international merchants.

CBD: Including Tianhe North, the Pearl River New Town and Guangzhou International Financial City.

Shopping streets: Beijing Lu Pedestrian Street, Shangxiajiu Pedestrian Street, Tee Mall.

Geography
Significance of city: International merchants center, China's third largest city.

Nearby cities: Dongguan (50 km/31 mi), Shenzhen (244 km/152 mi), Hong Kong (134 km/84 mi)

Municipality terrain: Pearl River Delta and low mountains with the South China Sea as the southern boundary

Main rivers: Pearl River

Transportation
Guangzhou Baiyun International Airport is one of the three national international aviation hubs, one of the Belt and Road Initiative, the Air Silk Road important international hub, and holds a core position at Guangdong-Hong Kong-Macao Greater Bay Area aviation hubs.

- 8 subway lines cover a total length of 236 km (147 mi)
- 2 central ring roads
- 4 regular rail lines

The Guangzhou High-Speed Railway covers 980 km (610 mi) at an average speed of 320 km/h.

(For information about transportation to conference hotel/venue, please refer to Pages 6-7)

For more information to plan your stay in Guangzhou, please visit :
https://www.chinahighlights.com/guangzhou/

GUANGZHOU ATTRACTIONS

Canton Tower
https://www.cantontower.com

Guangzhou Museum Of Art
https://gzam.com.cn/index.aspx

South China National Botanical Garden
http://scbg.cas.cn/

Guangzhou Shamian Island
http://en.wikipedia.org/w/index.php?title=Shamian_Island

Chimelong, Guangzhou
https://www.chimelong.com/gz/

Haizhu National Wetland Park
http://ehaizhu.shidicn.com/

Sun Yat-sen Memorial Hall
http://www.zs-hall.cn/

Nansha Wetland Park
http://gznssd.com.cn/

For more information, please visit: *https://www.gz.gov.cn/zlgz/index.html*

AIRPORT TRANSFER

From Guangzhou Baiyun International Airport to Conference Venue and Hotel, you can take :

- **Metro** *https://cs.gzmtr.com/ckfwEnglish/*

  appx 51 mins, cost around 7 CNY (about 0.97 USD or 0.89 EUR)

  1. Go to Terminal 1 or 2, and enter Airport S. Station of Guangzhou Metro Line 3.
  2. Transfer to Line 2 at Jiahewanggang Station towards Guangzhou South Railway Station.
  3. Get off at Yuexiu Park Station from Exit D1. China Hotel is on the left of Exit D1.

- **Taxi**

  appx 40 mins, cost around 100 CNY (about 13.80 USD or 12.69 EUR)

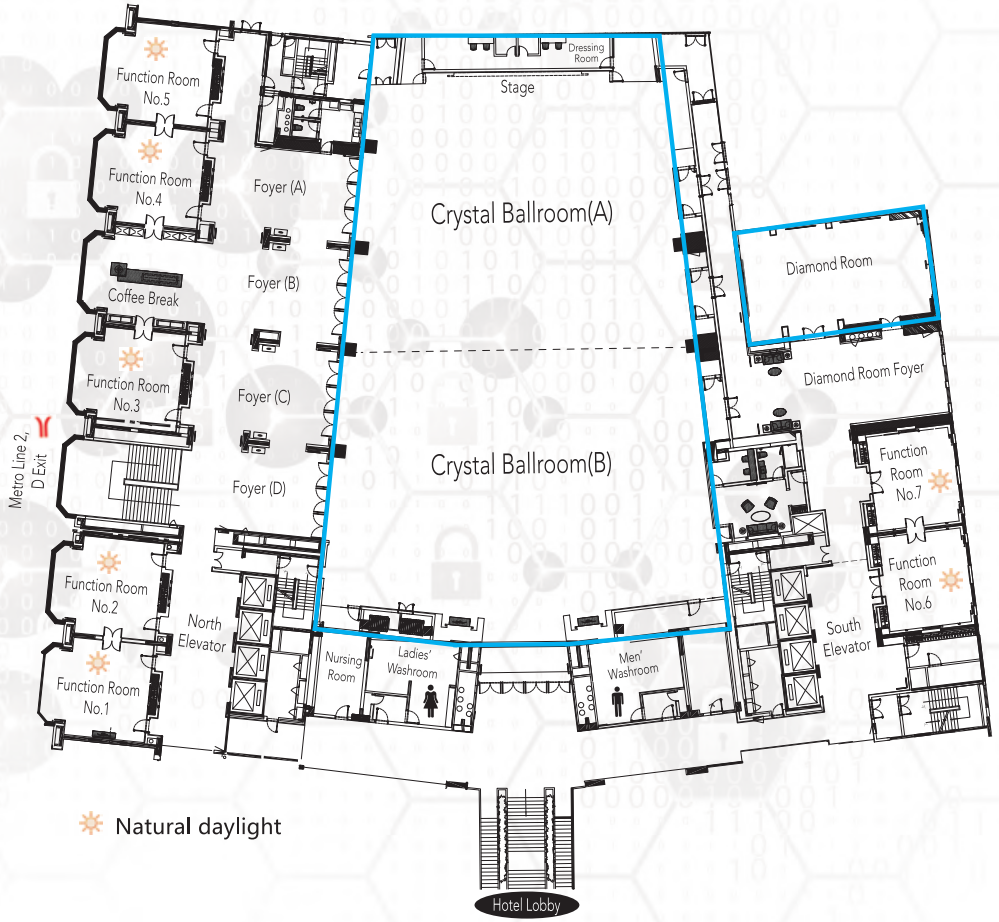
  Show the taxi driver the following paragraph:
  广东省广州市越秀区流花路122号中国大酒店

For more information, please visit: *https://asiacrypt.iacr.org/2023/travel.php*

CONFERENCE VENUE/ HOTEL

Conference Venue and Hotel
China Hotel 中国大酒店
122 Liuhua Road, Yuexiu District, Guangzhou, Guangdong China
中国广东省广州市越秀区流花路122号
Line 2 - Yuexiu Park Station, Exit D1（2号线 地铁越秀公园 D1 出口）

Tel : 86(20)8666 6888 *https://chinahotelgz.com/*



PROGRAM （Conference Venue : 2F China Hotel 中国大酒店）

Name Badge

Please wear your Asiacrypt 2023 name badge throughout the conference.

Track - Venue

- Track 1 - Crystal Ballroom(A) 丽晶殿A厅
- Track 2 - Crystal Ballroom(B) 丽晶殿B厅
- Track 3 - Diamond Room 钻石厅

Monday, December 4 2023 (Guangzhou)		
17:00-18:30	Registration	*(Hotel Lobby)*
18:00-20:30	Reception	*(4F Swimming Pool Side Welcome Cocktail Party)*

Tuesday, December 5 2023 (Guangzhou)		
8:00-9:00	Registration	*(Hotel Lobby)*
9:00-9:15	Opening remarks	*(Crystal Ballroom)*
9:15-10:15 Session Chair : Jian Guo	**Invited Talk 1: Xiaoyun Wang** Lattice-based Cryptography: From Theory to Practice	***(Crystal Ballroom)***
10:15-10:45	Coffee Break	
10:45-12:25		
Track 1 Anonymity 1 Session Chair : Jan Bobolz	Anonymous Counting Tokens *Fabrice Benhamouda, Mariana Raykova, Karn Seth* Predicate Aggregate Signatures and Applications *Tian Qiu, Qiang Tang* Short Concurrent Covert Authenticated Key Exchange (Short cAKE) *Karim Eldefrawy, Nicholas Genise, Stanislaw Jarecki* Bicameral and Auditably Private Signatures *Khoa Nguyen, Partha Sarathi Roy, Willy Susilo, Yanhong Xu*	
Track 2 Symmetric-Key Cryptanalysis 1 Session Chair : Guozhen Liu	Forgery Attacks on Several Beyond-Birthday-Bound Secure MACs *Yaobin Shen, François-Xavier Standaert, Lei Wang* Correlation Cube Attack Revisited:Improved Cube Search and Superpoly Recovery Techniques *Jianhua Wang, Lu Qin, Baofeng Wu* Differential-Linear Approximation Semi-Unconstrained Searching and Partition Tree: Application to LEA and Speck *Yi Chen, Zhenzhen Bao, Hongbo Yu* Cryptanalysis of Elisabeth-4 *Henri Gilbert, Rachelle Heim Boissier, Jérémy Jean, Jean-René Reinhard*	

Track 3 Functional Encryption 1 Session Chair : Duong Hieu Phan	Registered ABE via Predicate Encodings *Ziqi Zhu, Kai Zhang, Junqing Gong, Haifeng Qian* Registered (Inner-Product) Functional Encryption *Danilo Francati, Daniele Friolo, Monosij Maitra, Giulio Malavolta, Ahmadreza Rahimi, Daniele Venturi* Robust Decentralized Multi-Client Functional Encryption: Motivation, Definition, and Inner-Product Constructions *Yamin Li, Jianghong Wei, Fuchun Guo,Willy Susilo, Xiaofeng Chen* Cuckoo Commitments: Registration-Based Encryption and Key-Value Map Commitments for Large Spaces *Dario Fiore, Dimitris Kolonelos, Paola de Perthuis*	
12:25-14:00	Lunch	*(1F Food Street / 2F Cafe Veranda)*
14:00-15:40		
Track 1 Anonymity 2 Session Chair : Xinyi Huang	Threshold Structure-Preserving Signatures *Elizabeth Crites, Markulf Kohlweiss, Bart Preneel, Mahdi Sedaghat, Daniel Slamanig* Practical Round-Optimal Blind Signatures in the ROM from Standard Assumptions *Shuichi Katsumata, Michael Reichle, Yusuke Sakai* A Generic Construction of an Anonymous Reputation System and Instantiations from Lattices *Johannes Blömer, Jan Bobolz, Laurens Porzenheim* Universally Composable Auditable Surveillance *Valerie Fetzer, Michael Klooß, Jörn Müller-Quae, Markus Raiber, Andy Rupp*	
Track 2 Symmetric-Key Cryptanalysis 2 Session Chair : Thomas Peyrin	Algebraic Attacks on Round-Reduced Rain and Full AIM-III *Kaiyi Zhang, Qingju Wang, Yu Yu, Chun Guo, Hongrui Cui* Quantum Speed-Up for Multidimensional (Zero Correlation) Linear Distinguishers *Akinori Hosoyamada* Exact Security Analysis of ASCON *Bishwajit Chakraborty, Chandranan Dhar, Mridul Nandi*	

Track 3 Quantum Random Oracle Model Session Chair : Pierrick Méaux	On the (Im)possibility of Time-Lock Puzzles in the Quantum Random Oracle Model *Abtin Afshar, Kai-Min Chung, Yao-Ching Hsieh, Yao-Ting Lin, Mohammad Mahmoody* Towards compressed permutation oracles *Dominique Unruh* Tighter Security for Generic Authenticated Key Exchange in the QROM *Jiaxin Pan, Benedikt Wagner, Runzhi Zeng* Post-Quantum Security of Key Encapsulation Mechanism against CCA Attacks with a Single Decapsulation Query *Haodong Jiang, Zhi Ma, Zhenfeng Zhang*
15:40-16:10	Coffee Break
16:10-17:50	
Track 1 Key Exchange Session Chair : Kaitai Liang	Generalized Fuzzy Password-Authenticated Key Exchange from Error Correcting Codes *Jonathan Bootle, Sebastian Faller, Julia Hese, Kristina Hostáková, Johannes Ottenhues* A Generic Construction of Tightly Secure Password-based Authenticated Key Exchange *Jiaxin Pan, Runzhi Zeng* An Efficient Strong Asymmetric PAKE Compiler Instantiable from Group Actions *Jiayu Xu, Ian McQuoid* New SIDH Countermeasures for a More Efficient Key Exchange *Andrea Basso, Tako Boris Fouotsa*
Track 2 Quantum Cryptography & Quantum Cryptanalysis Session Chair : Xiaoyang Dong	Oblivious Transfer from Zero-Knowledge Proofs, Or How to Achieve Round-Optimal Quantum Oblivious Transfer and Zero-Knowledge Proofs on Quantum States *Léo Colisson, Garazi Muguruza, Florian Speelman* On the (Im)plausibility of Public-Key Quantum Money from Collision-Resistant Hash Functions *Prabhanjan Ananth, Zihan Hu, Henry Yuen* Improved Quantum Circuits for AES: Reducing the Depth and the Number of Qubits *Qun Liu, Bart Preneel, Zheng Zhao, Meiqin Wang*

Track 3 Zero-Knowledge Proofs – Foundations Session Chair : Moti Yung	Weak Zero-Knowledge via the Goldreich-Levin Theorem *Dakshita Khurana, Giulio Malavolta, Kabir Tomer* A Simple and Efficient Framework of Proof Systems for NP *Yuyu Wang, Chuanjie Su, Jiaxin Pan, Yu Chen* Sigma Protocols from Verifiable Secret Sharing and Their Applications *Min Zhang, Yu Chen, Chuanzhou Yao, Zhichao Wang*

Wednesday, December 6 2023 (Guangzhou)

9:00-10:15 Session Chair : Ron Steinfeld	**Award Papers** *(Crystal Ballroom)* On Gaussian Sampling, Smoothing Parameter and Application to Signatures *Thomas Espitau, Alexandre Wallet, Yang Yu* Exploiting the Symmetry of $\mathbb{Z}^n$: Randomization and the Automorphism Problem *Kaijie Jiang, Anyu Wang, Hengyi Luo, Guoxiao Liu, Yang Yu, Xiaoyun Wang* Exploiting Algebraic Structure in Probing Security *Maxime Plancon*
10:15-10:45	Coffee Break
10:45-12:25	
Track 1 Lattice-Based Signatures & Elliptic-Curve Cryptography Session Chair : Yang Yu	Antrag: Annular NTRU Trapdoor Generation *Thomas Espitau, Thi Thu Quyen Nguyen, Chao Sun, Mehdi Tibouchi, Alexandre Wallet* G+G: A Fiat-Shamir Lattice Signature Based on Convolved Gaussians *Julien Devevey, Alain Passelègue, Damien Stehlé* Cryptographic Smooth Neighbors *Giacomo Bruno, Maria Corte-Real Santos, Craig Costello, Jonathan Komada Eriksen, Michael Meyer, Michael Naehrig, Bruno Sterner* Non-Interactive Commitment from Non-Transitive Group Actions *Giuseppe D'Alconzo, Andrea Flamini, Andrea Gangemi*

Track 2 Searchable Encryption & Updatable Encryption Session Chair : Xiuhua Wang	Injection-Secure Structured and Searchable Symmetric Encryption *Ghous Amjad, Seny Kamara, Tarik Moataz* Hermes: I/O-Efficient Forward-Secure Searchable Symmetric Encryption *Brice Minaud, Michael Reichle* Efficient Updatable Public-Key Encryption from Lattices *Calvin Abou Haidar, Damien Stehlé, Alain Passelègue* CCA-1 Secure Updatable Encryption with Adaptive Security *Huanhuan Chen, Yao Jiang Galteland, Kaitai Liang*
Track 3 MPC for General Functionalities 1 & Functional Encryption 2 Session Chair : Junqing Gong	Robust Publicly Verifiable Covert Security: Limited Information Leakage and Guaranteed Correctness with Low Overhead *Yi Liu, Junzuo Lai, Qi Wang, Xianrui Qin, Anjia Yang, Jian Weng* Ramp hyper-invertible matrices and their applications to MPC protocols *Hongqing Liu, Chaoping Xing, Yanjiang Yang, Chen Yuan* Improved Fully Adaptive Decentralized MA-ABE for NC1 from MDDH *Jie Chen, Qiaohan Chu, Ying Gao, Jianting Ning, Luping Wang* Verifiable Decentralized Multi-Client Functional Encryption for Inner Product *Dinh Duy Nguyen, Duong Hieu Phan, David Pointcheval*
12:25-13:45	Lunch *(1F Food Street / 2F Cafe Veranda)*
13:45-15:00	
Track 1 Threshold Cryptography & Distributed Broadcast Session Chair : Qiang Tang	Simple Threshold (Fully Homomorphic) Encryption From LWE With Polynomial Modulus *Katharina Boudgoust, Peter Scholl* VSS from Distributed ZK Proofs and Applications *Shahla Atapoor, Karim Baghery, Daniele Cozzo, Robi Pedersen* Threshold Linear Secret Sharing to the Rescue of MPC-in-the-Head *Thibauld Feneuil, Matthieu Rivain* Distributed Broadcast Encryption from Bilinear Groups *Dimitris Kolonelos, Giulio Malavolta, Hoeteck Wee*

Track 2 Side-Channels & Public-key Cryptanalysis Session Chair : Alexandre Wallet	SCA-LDPC: A Code-Based Framework for Key-Recovery Side-Channel Attacks on Post-Quantum Encryption Schemes *Qian Guo, Denis Nabokov, Alexander Nilsson, Thomas Johansson* Practically Efficient Private Set Intersection From Trusted Hardware with Side-Channels *Felix Dörre, Jeremias Mechler, Jörn Müller-Quade* Quantitative Fault Injection Analysis *Jakob Feldtkeller, Tim Gueneysu, Patrick Schaumont* We Are on the Same Side. Alternative Sieving Strategies for the Number Field Sieve *Charles Bouillaguet, Ambroise Fleury, Pierre-Alain Fouque, Paul Kirchner*
Track 3 Functional Commitments and Proofs & MPC Session Chair : Khoa Nguyen	Zero-Knowledge Functional Elementary Databases *Xinxuan Zhang, Yi Deng* LERNA: Secure Single-Server Aggregation via Key-Homomorphic Masking *Hanjun Li, Huijia Lin, Antigoni Polychroniadou, Stefano Tessaro* Non-Interactive Zero-Knowledge Functional Proofs *Gongxian Zeng, Junzuo Lai, Zhengan Huang, Linru Zhang, Xiangning Wang, Kwok-Yan Lam, Huaxiong Wang, Jian Weng*
15:25-15:55	Coffee Break
15:55-17:35	
Track 1 Fully Homomorphic Encryption Session Chair : Alain Passelègue	Amortized Bootstrapping Revisited: Simpler, Asymptotically-faster, Implemented *Antonio Guimarães, Hilder V. L. Pereira, Barry van Leeuwen* Rotation Key Reduction for Client-Server Systems of Deep Neural Network on Fully Homomorphic Encryption *Joon-Woo Lee, Eunsang Lee, Young-Sik Kim, Jong-Seon No* Homomorphic Polynomial Evaluation using Galois Structure and Applications to BFV Bootstrapping *Hiroki Okada, Rachel Player, Simon Pohmann* Amortized Functional Bootstrapping in less than 7ms, with ~O(1) polynomial multiplications *Zeyu Liu, Yunhao Wang*

Track 2 Quantum Cryptanalysis Session Chair : Zhenzhen Bao	Quantum Attacks on Hash Constructions with Low Quantum Random Access Memory *Xiaoyang Dong, Shun Li, Phuong Pham, Guoyan Zhang* On Quantum Secure Compressing Pseudorandom Functions *Ritam Bhaumik, Benoît Cogliati, Jordan Ethan, Ashwin Jha* Hidden Stabilizers, the Isogeny To Endomorphism Ring Problem and the Cryptanalysis of pSIDH *Péter Kutas, Christophe Petit, Gábor Ivanyos, Mingjie Chen, Antonin Leroux, Muhammad Imran* Concrete Analysis of Quantum Lattice Enumeration *Shi Bai, Maya-Iggy van Hoof, Floyd B. Johnson, Tanja Lange, Tran Ngo*
Track 3 Security Models Session Chair : Chun Guo	Unified View for Notions of Bit Security *Shun Watanabe, Kenji Yasunaga* The Relationship Between Idealized Models Under Computationally Bounded Adversaries *Cong Zhang, Mark Zhandry* Just How Fair is an Unreactive World? *Srinivasan Raghuraman, Yibin Yang*
18:30-21:00	Dinner Reception *(Crystal Ballroom)*
19:30-22:00 Session Chair : Kang Yang and Yu Yu	Rump Session *(Crystal Ballroom)*

Thursday, December 7 2023 (Guangzhou)

9:00-10:00 Session Chair : Ron Steinfeld	**Invited talk 2: Mehdi Tibouchi** ***(Crystal Ballroom)*** Mathematical Problems arising from Timing Attacks on Signatures and their Countermeasures
10:00-10:30	Coffee Break
10:30-12:10	
Track 1 Symmetric Key Cryptanalysis - Automated Tools Session Chair : Meicheng Liu	Automated Meet-in-the-Middle Attack Goes to Feistel *Qingliang Hou, Lingyue Qin, Xiaoyang Dong, Guoyan Zhang, Xiaoyun Wang* Revisiting Higher-Order Differential-Linear Attacks from an Algebraic Perspective *Kai Hu, Thomas Peyrin, Quan Quan Tan, Trevor Yap Hong Eng* More Insight on Deep Learning-aided Cryptanalysis *Zhenzhen Bao, Jinyu Lu, Yiran Yao, Liu Zhang*

Track 2 Cryptanalysis of Post-Quantum Cryptography Session Chair : Thomas Espitau	A New Approach based on Quadratic Forms to Attack the McEliece Cryptosystem *Alain Couvreur, Rocco Mora, Jean-Pierre Tillich* Solving the Hidden Number Problem for CSIDH and CSURF via Automated Coppersmith *Jonas Meers, Julian Nowakowski* Memory-Efficient Attacks on Small LWE Keys *Andre Esser, Rahul Girme, Arindam Mukherjee, Santanu Sarkar* Too Many Hints - When LLL Breaks LWE *Alexander May, Julian Nowakowski*
Track 3 Zero-Knowledge Proofs – Succinctness Session Chair : Kang Yang	Fiat-Shamir Security of FRI and Related SNARKs *Alexander R. Block, Albert Garreta, Jonathan Katz, Justin Thaler, Pratyush Ranjan Tiwari, Michał Zając* On Black-Box Knowledge-Sound Commit-And-Prove SNARKs *Helger Lipmaa* Protostar: Generic Efficient Accumulation/Folding for Special-sound Protocols *Benedikt Bünz, Binyi Chen* Polynomial IOPs for Memory Consistency Checks in Zero-Knowledge Virtual Machines *Yuncong Zhang, Shi-Feng Sun, Ren Zhang, Dawu Gu*
12:10-13:30	Lunch *(1F Food Street / 2F Cafe Veranda)*
13:30-14:45	
Track 1 Real-World Protocols Session Chair : Seth Karn	To Attest or not to Attest, This is the Question – Provable Attestation in FIDO2 *Nina Bindel, Nicolas Gama, Sandra Guasch, Eyal Ronen* WhatsUpp with Sender Keys? Analysis, Improvements and Security Proofs *David Balbás, Daniel Collins, Phillip Gajland* The Pre-Shared Key Modes of HPKE *Joël Alwen, Jonas Janneck, Eike Kiltz, Benjamin Lipp*

Track 2 Code-Based Cryptography Session Chair : Andre Esser	Pseudorandomness of Decoding, Revisited: Adapting OHCP to Code-Based Cryptography *Maxime Bombar, Alain Couvreur, Thomas Debris-Alazard* Blockwise Rank Decoding Problem and LRPC Codes: Cryptosystems with Smaller Sizes *Yongcheng Song, Jiang Zhang, Xinyi Huang, Wei Wu* SDitH in the QROM *Andreas Huelsing, Carlos Aguilar-Melchor, David Joseph, Christian Majenz, Eyal Ronen, Dongze Yue* A New Formulation of the Linear Equivalence Problem and Shorter LESS Signatures *Edoardo Persichetti, Paolo Santini*
Track 3 MPC for General Functionalities 2 Session Chair : Siu Ming Yiu	Degree-D Reverse Multiplication-Friendly Embeddings: Constructions and Applications *Daniel Escudero, Cheng Hong, Hongqing Liu, Chaoping Xing, Chen Yuan* Adaptive Distributional Security for Garbling Schemes with O(|x|) Online Complexity *Estuardo Alpirez Bock, Chris Brzuska, Pihla Karanko, Sabine Oechsner, Kirthivaasan Puniamurthy* MPC With Delayed Parties Over Star-Like Networks *Mariana Gama, Emad Heydari Beni, Emmanuela Orsini, Nigel Smart, Oliver Zajonc*
14:45-15:45	IACR Membership Meeting *(Crystal Ballroom - A)*
15:45-19:00	Free Afternoon
19:00-21:30	Banquet *(Entry begins at 18:30 - Crystal Ballroom)*

Friday, December 8 2023 (Guangzhou)

9:00-10:15	
Track 1 Public-Key Encryption - Special Functionalities Session Chair : Wouter Castryck	Sender-Anamorphic Encryption Reformulated: Achieving Robust and Generic Constructions *Yi Wang, Rongmao Chen, Xinyi Huang, Moti Yung* Efficient Secure Storage with Version Control and Key Rotation *Long Chen, Hui Guo, Ya-Nan Li, Qiang Tang* Fine-Grained Proxy Re-Encryption: Definitions & Constructions from LWE *Yunxiao Zhou, Shengli Liu, Shuai Han, Haibin Zhang*
Track 2 Symmetric-Key – Design Session Chair : Yaobin Shen	The Indifferentiability of the Duplex and its Practical Applications *Jean Paul Degabriele, Marc Fischlin, Jérôme Govinden* Populating the Zoo of Rugged Pseudorandom Permutations *Jean Paul Degabriele, Vukašin Karadžić* Generic Security of the SAFE API and Its Applications *Dmitry Khovratovich, Mario Marhuenda Beltrán, Bart Mennink*
Track 3 MPC for Specific Functionalities Session Chair : Karim Baghery	Scalable Multi-party Private Set Union from Multi-Query Secret-Shared Private Membership Test *Xiang Liu, Ying Gao* Lattice-Based Functional Commitments: Fast Verification and Cryptanalysis *Hoeteck Wee, David J. Wu* Unconditionally Secure Multiparty Computation for Symmetric Functions with Low Bottleneck Complexity *Reo Eriguchi*
10:15-10:45	Coffee Break
10:45-12:00	
Track 1 Post-Quantum Encryption Session Chair : Edoardo Persichetti	FESTA: Fast Encryption from Supersingular Torsion Attacks *Andrea Basso, Luciano Maino, Giacomo Pope* A Polynomial Time Attack on Instances of M-SIDH and FESTA *Wouter Castryck, Frederik Vercauteren* NEV: Faster and Smaller NTRU Encryption using Vector Decoding *Jiang Zhang, Dengguo Feng, Di Yan*
Track 2 Secure Two-Party Computation Session Chair : Yuncong Hu	Breaking the Size Barrier: Universal Circuits meet Lookup Tables *Yann Disser, Daniel Günther, Thomas Schneider, Maximilian Stillger, Arthur Wigandt, Hossein Yalame* Amortized NISC over $\mathbb{Z}_{2^k}$ from RMFE *Fuchun Lin, Chaoping Xing, Yizhou Yao, Chen Yuan* Two-Round Concurrent 2PC from Sub-Exponential LWE *Behzad Abdolmaleki, Saikrishna Badrinarayanan, Rex Fernando, Giulio Malavolta, Ahmadreza Rahimi, Amit Sahai*
12:00-12:10	Closing remarks *(Crystal Ballroom - A)*
12:10-14:00	Lunch *(2F Cafe Veranda)*