Kai-Min Chung

Institute of Information Science, Academia Sinica
Room 716 New Building
No 128, Academia Road, Section 2
Nankang, Taipei 11529, Taiwan

886-2-2788-3799 #1716
kmchung@as.edu.tw
http://www.iis.sinica.edu.tw/pages/kmchung/
http://www.iis.sinica.edu.tw/~kmchung/

Current Position

Distinguished Research Fellow Aug. 2024 – Present
Institute of Information Science, Academia Sinica, Taiwan

Deputy Director Jul. 2024 – Present
Institute of Information Science, Academia Sinica, Taiwan

Previous Position

Research Fellow Feb. 2020 – Aug. 2024
Institute of Information Science, Academia Sinica, Taiwan

Associate Research Fellow Mar. 2015 – Feb. 2020
Institute of Information Science, Academia Sinica, Taiwan

Assistant Research Fellow Sep. 2013 – Mar. 2015
Institute of Information Science, Academia Sinica, Taiwan

Postdoctoral Research Associate Aug. 2010 – Aug. 2013
Cornell University, Ithaca NY, USA

- Advisor: Rafael Pass
- *Simons Postdoctoral Fellowship (Aug. 2010 – Aug. 2012)*

Education

Harvard University, Cambridge MA, USA
Ph.D. in Computer Science Sep. 2005 – Mar. 2011

- Advisor: Salil P. Vadhan
- Thesis: *Efficient Parallel Repetition Theorems with Applications to Security Amplification*

National Taiwan University, Taipei, Taiwan
Bachelor of Science in Engineering Sep. 1999 – Jun. 2003

- Major: Computer Science & Information Engineering; Minor: Mathematics

Research Interests

Quantum Cryptography, Quantum Complexity Theory, and Quantum Program Verification

Honors and Awards

NSTC Outstanding Research Award (FY112) 2024

PLDI 2023 Distinguished Paper Award 2023
for paper "An Automata-based Framework for Verification and Bug Hunting in Quantum Circuits" (with Yu-Fang Chen, Ondřej Lengál, Jyun-Ao Lin, Wei-Lun Tsai, and Di-De Yen)

MOST Outstanding Research Award (FY109) 2021

Academia Sinica Investigator Award 2021
associated with five years of funding for research on "Theoretical Exploration in Quantum Cryptography"

Academia Sinica Research Award for Junior Research Investigators 2020

MOST Ta-You Wu Memorial Award 2018

FAOS Young Scholar Creative Research Award 2017

Academia Sinica Career Development Award 2016
associated with five years of funding for research on "Crypto for Modern Cloud Architecture and Post-quantum Crypto against Quantum Side-Info"

SYNERGISTIC ACTIVITIES

Steering and Advisory Committees

- International Symposium on Algorithms and Computation (**ISAAC**)
  Advisory Committee Jan. 2026 - present
- Annual International Conference on The Theory and Application of Cryptology and Information Security (**ASIACRYPT**)
  Steering Committee Dec. 2023 - present
- Conference on the Theory of Quantum Computation, Communication and Cryptography (**TQC**)
  Steering Committee Nov. 2023 - present
- International Conference on Quantum Cryptography (**QCrypt**)
  Steering Committee Sep. 2021 - Sep. 2026

Program Chair

- 30th Annual International Conference on the Theory and Applications of Cryptology and Information Security (Asiacrypt 2024)
- 4th Information-Theoretic Cryptography conference (ITC 2023)

Program Committee

- General Theory
  STOC '22, **FOCS** '22
- Cryptography
  CRYPTO '26, '25, '23, '19, '13, **EUROCRYPT** '26, '21, '19, **ASIACRYPT** '23 (Area Chair), '21, '17, '15, '14, **TCC** '26, '25, '20, '19, '17, '16, '15, '14, **PKC** '20, '18, **ITC** '22, '21, '20, **TQC** '22
- Quantum
  QIP '23, **QCrypt** '18
- Complexity
  CCC '17

- Algorithm
  ISAAC '18, '15
- Programming Languages
  PLDI '27

General Chair

- 30th International Conference on Practice and Theory of Public-Key Cryptography (PKC 2027)
- 15th Real World Crypto Symposium (RWC 2026)
- 16th International Conference on Post-Quantum Cryptography (PQC 2025)
- 25th Workshop on Elliptic Curve Cryptography (ECC 2024)
- 21st IACR Theory of Cryptography Conference (TCC 2023)
- 28th Annual International Conference on The Theory and Application of Cryptology and Information Security (Asiacrypt 2022)
- 12th International Conference on Quantum Cryptography (QCrypt 2022)
- 19th International Conference on the Theory and Practice of Public-Key Cryptography (PKC 2016)

Conference Chair

- 36th International Symposium on Algorithms and Computation (ISAAC 2025)

Organizing Committee

- 36th International Symposium on Algorithms and Computation (ISAAC 2025)
- 27th Conference on Quantum Information Processing (QIP 2024)
- 16th Asian Quantum Information Science Conference (AQIS 2016)

Journal Editors

- IACR Communications in Cryptology (CiC Area Editor) Jan. 2024 - Dec. 2025
- ACM Computing Surveys (CSUR Associate Editor) Nov. 2021 - Nov. 2024
- ACM Transactions on Computation Theory (ToCT Associate Editor) Jan. 2021 - present
- Journal of Information Science and Engineering (JISE Associate Editor) Jan. 2020 - present

Association Director

- Taiwan Association of Quantum Computation and Information Technology Nov. 2020 - present
- Algorithm and Computation Theory Association (ACTA) Feb. 2020 - Dec. 2021

International Advisory Committee

- One-month Workshop on Quantum Information and String Theory, Yukawa Institute for Theoretical Physics (YITP), Kyoto University May–June, 2027

Scientific Committee

- Advances in Quantum Cryptography, Institut Henri Poincaré (IHP), Paris Sep to Dec, 2027

GRANTS

Zero-Knowledge Proofs in the Quantum World 2026-2029
Funded by National Science and Technology Council, Taiwan.
(No: 115-2221-E-001-002-MY3)

Interdisciplinary Research On Quantum CS: Cryptography, Program Verification, and Their Interplay 2023-2027
Funded by Air Force Office of Scientific Research (AFOSR), USA.
PI: Kai-Min Chung and Yu-Fang Chen

Theoretical Development in Quantum Computer Science 2022-2027
Funded by National Science and Technology Council, Taiwan.
PI: Kai-Min Chung, Shih-Han Hung, Han-Hsuan Lin, Jyun-Ao Lin, Bo-Yin Yang, and Yu-Fang Chen
(No: 111-2119-M-001-004, 112-2119-M-001-006, 113-2119-M-001-009, 114-2119-M-001-002, 115-2119-M-001-002)

Academia Sinica 2021 Investigator Award 2021-2025
Funded by Academia Sinica, Taiwan.

Cryptography, a Challenge in the Age of Quantum Computing 2021-2024
Funded by Academia Sinica, Taiwan.
PI: Bo-Yin Yang, Kai-Min Chung, and Bow-Yaw Wang

Secure Multiparty Quantum Computation 2020-2022
Funded by Air Force Office of Scientific Research (AFOSR), USA.

Theoretical Challenges and Opportunities in Post-Quantum Cryptography 2020-2023
Funded by Ministry of Science and Technology, Taiwan.
(No: 109-2223-E-001-001-MY3)

Silicon-based quantum devices, quantum computing and quantum communication
Sub-project 4: Quantum communication and cryptography 2018-2022
Funded by Ministry of Science and Technology, Taiwan.
(No: 107-2627-E-002-002)

Crypto for Modern Cloud Architecture 2017-2020
Funded by Ministry of Science and Technology, Taiwan.
(No: 106-2628-E-001-002-MY3)

The Young Scholars' Creativity Award 2017-2019
Funded by Foundation for the Advancement of Outstanding Scholarship, Taiwan.

Academia Sinica 2016 Career Development Award 2016-2020
Funded by Academia Sinica, Taiwan.

Li Foundation Heritage Prize for "Excellence in Creativity" 2014-2015
Funded by The Li Foundation, Inc., USA.

Advancing New Age Cryptography—New Assumptions, Tasks, and Challenges 2014-2017
Funded by Ministry of Science and Technology, Taiwan.
(No: 103-2221-E-001-022-MY3)

CONFERENCE PUBLICATIONS

[79] *Complexity Theory for Quantum Promise Problems*
Nai-Hui Chia, Kai-Min Chung, Tzu-Hsiang Huang, Chuhan Lu, Jhih-Wei Shih
To appear in Proceedings of The 18th Innovations in Theoretical Computer Science (**ITCS**), 2027.
Contributed talk at The 21st Conference on the Theory of Quantum Computation, Communication and Cryptography (**TQC**), 2026.

[78] *Constant-Rate Certified Deletion*
Kai-Min Chung, Tzu-Hsiang Huang, Wei-Hsiang Hung, Shota Yamada
In Proceedings of The 46th International Cryptology Conference (**CRYPTO**), 2026.

[77] *The Black-Box Simulation Barrier Persists in a Fully Quantum World*
Nai-Hui Chia, Kai-Min Chung, Xiao Liang, Jiahui Liu
In Proceedings of The 45th International Conference on the Theory and Applications of Cryptographic Techniques (**EUROCRYPT**), 2026.
Contributed talk at The 21st Conference on the Theory of Quantum Computation, Communication and Cryptography (**TQC**), 2026.

[76] *Tight Quantum Time-Space Tradeoffs for Permutation Inversion*
Akshima, Tyler Besselman, Kai-Min Chung, Siyao Guo, Tzu-Yi Yang
In Proceedings of The 45th International Conference on the Theory and Applications of Cryptographic Techniques (**EUROCRYPT**), 2026.

[75] *Equivalence Checking of Quantum Circuits via Path-Sum and Weighted Model Counting*
Wei-Jia Huang, Christophe Chareton, Yu-Fang Chen, Kai-Min Chung, Min-Hsiu Hsieh, Alfons Laarman, Jingyi Mei
In Proceedings of The 32nd International Conference on Tools and Algorithms for the Construction and Analysis of Systems (**TACAS**), 2026.

[74] *AutoQ 2.0: From Verification of Quantum Circuits to Verification of Quantum Programs*
Yu-Fang Chen, Kai-Min Chung, Min-Hsiu Hsieh, Wei-Jia Huang, Ondřej Lengál, Jyun-Ao Lin, Wei-Lun Tsai
In Proceedings of The 31st International Conference on Tools and Algorithms for the Construction and Analysis of Systems (**TACAS**), 2025.

[73] *On Central Primitives for Quantum Cryptography with Classical Communication*
Kai-Min Chung, Eli Goldin, Matthew Gray
In Proceedings of The 44th International Cryptology Conference (**CRYPTO**), 2024.

[72] *Best-of-Both-Worlds Multiparty Quantum Computation with Publicly Verifiable Identifiable Abort*
Kai-Min Chung, Mi-Ying Huang, Er-Cheng Tang, and Jiapeng Zhang
In Proceedings of The 43rd Annual International Conference on the Theory and Applications of Cryptographic Techniques (**EUROCRYPT**), 2024.

[71] *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, and Mohammad Mahmoody
In Proceedings of The 29th Annual International Conference on the Theory and Applications of Cryptology and Information Security (**ASIACRYPT**), 2023.

[70] *AutoQ: An Automata-based Quantum Circuit Verifier*
Yu-Fang Chen , Kai-Min Chung, Ondřej Lengál, Jyun-Ao Lin, Wei-Lun Tsai, and Di-De Yen
In Proceedings of The 35th International Conference on Computer Aided Verification (**CAV**), 2023.

[69] *On the Impossibility of General Parallel Fast-forwarding of Hamiltonian Simulation*
Nai-Hui Chia, Kai-Min Chung, Yao-Ching Hsieh, Han-Hsuan Lin, Yao-Ting Lin, and Yu-Ching Shen
In Proceedings of The Computational Complexity Conference (**CCC**), 2023.

[68] *An Automata-based Framework for Verification and Bug Hunting in Quantum Circuits*
Yu-Fang Chen, Kai-Min Chung, Ondřej Lengál, Jyun-Ao Lin, Wei-Lun Tsai, and Di-De Yen
In Proceedings of The 44th ACM SIGPLAN Conference on Programming Language Design and Implementation (**PLDI**), 2023. *Distinguished Paper Award.*

[67] *Black-Box Separations for Non-interactive Classical Commitments in a Quantum World*
Kai-Min Chung, Yao-Ting Lin, and Mohammad Mahmoody
In Proceedings of The 42nd Annual International Conference on the Theory and Applications of Cryptographic Techniques (**EUROCRYPT**), 2023.

[66] *Collusion-Resistant Functional Encryption for RAMs*
Prabhanjan Ananth, Kai-Min Chung, Xiong Fan, and Luowen Qian
In Proceedings of the 28th Annual International Conference on the Theory and Applications of Cryptology and Information Security (**ASIACRYPT**), 2022.

[65] *On the Impossibility of Key Agreements from Quantum Random Oracles*
Per Austrin, Hao Chung, Kai-Min Chung, Shiuan Fu, Yao-Ting Lin, and Mohammad Mahmoody
In Proceedings of The 42nd International Cryptology Conference (**CRYPTO**), 2022.

[64] *Post-Quantum Simulatable Extraction with Minimal Assumptions: Black-Box and Constant-Round*
Nai-Hui Chia, Kai-Min Chung, Xiao Liang, and Takashi Yamakawa
In Proceedings of The 42nd International Cryptology Conference (**CRYPTO**), 2022.

[63] *Constant-round Blind Classical Verification of Quantum Sampling*
Kai-Min Chung, Yi Lee, Han-Hsuan Lin, and Xiaodi Wu
In Proceedings of The 41st Annual International Conference on the Theory and Applications of Cryptographic Techniques (**EUROCRYPT**), 2022.

[62] *A Note on the Post-Quantum Security of (Ring) Signatures*
Rohit Chatterjee, Kai-Min Chung, Xiao Liang, and Giulio Malavolta
In Proceedings of The 25th Practice and Theory of Public-Key Cryptography (**PKC**), 2022.

[61] *On the Impossibility of Post-Quantum Black-Box Zero-Knowledge in Constant Rounds*
Nai-Hui Chia, Kai-Min Chung , Qipeng Liu, and Takashi Yamakawa
In Proceedings of The 62nd Annual IEEE Symposium on Foundations of Computer Science (**FOCS**), 2021.
Contributed talk at the 11th International Conference on Quantum Cryptography (**QCrypt**), 2021.
- Merged with Black-Box Approach to Post-Quantum Zero-Knowledge in Constant Round

Contributed talk at the 25th Annual Conference on Quantum Information Processing (**QIP**), 2022.
- Merged with Black-Box Approach to Post-Quantum Zero-Knowledge in Constant Round

[60] *On the Concurrent Composition of Quantum Zero-Knowledge*
Prabhanjan Ananth, Kai-Min Chung, and Rolando L. La Placa
In Proceedings of The 41st International Cryptology Conference (**CRYPTO**), 2021.

[59] *Round Efficient Secure Multiparty Quantum Computation with Identifiable Abort*
Bar Alon, Hao Chung, Kai-Min Chung, Mi-Ying Huang, Yi Lee, and Yu-Ching Shen
In Proceedings of The 41st International Cryptology Conference (**CRYPTO**), 2021.

[58] *Game-Theoretic Fairness Meets Multi-Party Protocols: The Case of Leader Election*
Kai-Min Chung, T-H. Hubert Chan, Ting Wen, and Elaine Shi
In Proceedings of The 41st International Cryptology Conference (**CRYPTO**), 2021.

[57] *A Black-Box Approach to Post-Quantum Zero-Knowledge in Constant Rounds*
Nai-Hui Chia, Kai-Min Chung, and Takashi Yamakawa
In Proceedings of The 41st International Cryptology Conference (**CRYPTO**), 2021.

[56] *Sample Efficient Algorithms for Learning Quantum Channels in PAC Model and the Approximate State Discrimination Problem*
Kai-Min Chung and Han-Hsuan Lin
In Proceedings of The 16th Conference on the Theory of Quantum Computation, Communication and Cryptography (**TQC**), 2021.

[55] *On the Compressed-Oracle Technique, and Post-Quantum Security of Proofs of Sequential Work*
Kai-Min Chung, Serge Fehr, Yu-Hsuan Huang, and Tai-Ning Liao
In Proceedings of The 40th Annual International Conference on the Theory and Applications of Cryptographic Techniques (**EUROCRYPT**), 2021.
Contributed talk at the 11th International Conference on Quantum Cryptography (**QCrypt**), 2021.

[54] *Classical Verification of Quantum Computations with Efficient Verifier*
Nai-Hui Chia, Kai-Min Chung, and Takashi Yamakawa
In Proceedings of The 18th Theory of Cryptography Conference (**TCC**), 2020.

[53] *Tight Quantum Time-Space Tradeoffs for Function Inversion*
Kai-Min Chung, Siyao Guo, Qipeng Liu, and Luowen Qian
In Proceedings of The 61st Annual IEEE Symposium on Foundations of Computer Science (**FOCS**), 2020.

[52] *On the Hardness of Massively Parallel Computation*
Kai-Min Chung, Kuan-Yi Ho, and Xiaorui Sun
In Proceedings of The 32nd ACM Symposium on Parallelism in Algorithms and Architectures (**SPAA**), 2020.

[51] *Lower Bounds for Function Inversion with Quantum Advice*
Kai-Min Chung, Tai-Ning Liao, and Luowen Qian
In Proceedings of The 1st Information-Theoretic Cryptography (**ITC**), 2020.

[50] *MPC for MPC: Secure Computation on a Massively Parallel Computing Architecture*
T-H. Hubert Chan, Kai-Min Chung, Wei-Kai Lin, and Elaine Shi
In Proceedings of The 11th Innovations in Theoretical Computer Science (**ITCS**), 2020.

[49] *On the Need for Large Quantum Depth*
Nai-Hui Chia, Kai-Min Chung, and Ching-Yi Lai
In Proceedings of The 52nd ACM Symposium on Theory of Computing (**STOC**), 2020.
Contributed talk at the 23rd Annual Conference on Quantum Information Processing(**QIP**), 2020.
The Journal of the ACM (**JACM**), 70(1), February 2023

[48] *Adaptively Secure Garbling Schemes for Parallel Computations*
Kai-Min Chung and Luowen Qian
In Proceedings of The 17th Theory of Cryptography Conference (**TCC**), 2019.

[47] *Interactive Leakage Chain Rule for Quantum Min-entropy,*
Kai-Min Chung and Ching-Yi Lai
In Proceedings of The 2019 IEEE International Symposium on Information Theory, 2019 (**ISIT**), 2019.

[46] *A Quantum-Proof Non-Malleable Extractor With Application to Privacy Amplification against Active Quantum Adversaries*
Divesh Aggarwal, Kai-Min Chung, Han-hsuan Lin, and Thomas Vidick
In Proceedings of The 38th Annual International Conference on the Theory and Applications of Cryptographic Techniques (**EUROCRYPT**), 2019.

[45] *On Quantum Advantage in Information Theoretic Single-Server PIR*
Dorit Aharonov, Zvika Brakerski, Kai-Min Chung, Ayal Green, Ching-Yi Lai, and Or Sattath
In Proceedings of The 38th Annual International Conference on the Theory and Applications of Cryptographic Techniques (**EUROCRYPT**), 2019.

[44] *Foundations of Differentially Oblivious Algorithms*
T-H. Hubert Chan, Kai-Min Chung, Bruce Maggs, and Elaine Shi
In Proceedings of ACM-SIAM Symposium on Discrete Algorithms (**SODA**), 2019.
The Journal of the ACM (**JACM**), 69(4), August 2022

[43] *On the Algorithmic Power of Spiking Neural Networks*
Chi-Ning Chou, Kai-Min Chung, Chi-Jen Lu
In Proceedings of The 10th Innovations in Theoretical Computer Science (**ITCS**), 2019.

[42] *Game Theoretic Notions of Fairness in Multi-Party Coin Toss*
Kai-Min Chung, Yue Guo, Wei-Kai Lin, Rafael Pass, and Elaine Shi
In Proceedings of the 16th Theory of Cryptography Conference (**TCC**), 2018.

[41] *On the Complexity of Simulating Auxiliary Input*
Yi-Hsiu Chen, Kai-Min Chung, and Jyun-Jie Liao
In Proceedings of the 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques (**EUROCRYPT**), 2018.

[40] *On the Depth of Oblivious Parallel RAM*
T-H. Hubert Chan, Kai-Min Chung, and Elaine Shi
In Proceedings of the 23rd Annual International Conference on the Theory and Applications of Cryptology and Information Security (**ASIACRYPT**), 2017.

[39] *Computational Notions of Quantum Min-Entropy*
Yi-Hsiu Chen, Kai-Min Chung, Ching-Yi Lai, Salil Vadhan, and Xiaodi Wu
Contributed talk at the 7th International Conference on Quantum Cryptography (**QCrypt**), 2017.

[38] *General Randomness Amplification with Non-signaling Security*
Kai-Min Chung, Yaoyun Shi, and Xiaodi Wu
Contributed talk at the 20th Annual Conference on Quantum Information Processing (**QIP**), 2017.

[37] *Delegating RAM Computations with Adaptive Soundness and Privacy*
Prabhanjan Ananth, Yu-Chi Chen, Kai-Min Chung, Huijia Lin, and Wei-Kai Lin
In Proceedings of the 14th Theory of Cryptography Conference (**TCC-B**), 2016.

[36] *Cryptography for Parallel RAM via Indistinguishability Obfuscation*
Yu-Chi Chen, Sherman S. M. Chow, Kai-Min Chung, Russell W. F. Lai, Wei-Kai Lin, and Hong-Sheng Zhou
In Proceedings of the 7th Innovations in Theoretical Computer Science (**ITCS**), 2016.

[35] *Oblivious Parallel RAM and Applications*
Elette Boyle, Kai-Min Chung, and Rafael Pass
In Proceedings of the 13th Theory of Cryptography Conference (**TCC-A**), 2016.

[34] *Large-Scale Secure Computation: Multi-party Computation for (Parallel) RAM Programs*
Elette Boyle, Kai-Min Chung, and Rafael Pass
In Proceedings of the 35th International Cryptology Conference (**CRYPTO**), 2015.

[33] *Constant-Round Concurrent Zero-knowledge from Indistinguishability Obfuscation*
Kai-Min Chung, Huijia Lin, and Rafael Pass
In Proceedings of the 35th International Cryptology Conference (**CRYPTO**), 2015.

[32] *Parallel Repetition for Entangled k-player Games via Fast Quantum Search*
Kai-Min Chung, Xiaodi Wu,and Henry S.Yuen
In Proceedings of the 30th Computational Complexity Conference (**CCC**), 2015.

[31] *Tight Parallel Repetition Theorems for Public-Coin Arguments using KL-divergence*
Kai-Min Chung and Rafael Pass
In Proceedings of the 12th Theory of Cryptography Conference (**TCC**), 2015.

[30] *From Weak to Strong Zero-Knowledge and Applications*
Kai-Min Chung, Edward Lui, and Rafael Pass
In Proceedings of the 12th Theory of Cryptography Conference (**TCC**), 2015.

[29] *Statistically-secure ORAM with $\tilde{O}(\log^2 n)$ Overhead*
Kai-Min Chung, Zhenming Liu, and Rafael Pass
In Proceedings of the 20th Annual International Conference on the Theory and Application of Cryptology and Information Security (**ASIACRYPT**), 2014.

[28] *On the Impossibility of Cryptography with Tamperable Randomness*
Per Austrin, Kai-Min Chung, Mohammad Mahmoody, Rafael Pass, and Karn Seth
Algorithmica, 79(4):1052-1101, December 2017
In Proceedings of the 34th International Cryptology Conference (**CRYPTO**), 2014.

[27] *Distributed Algorithms for the Lovasz Local Lemma and Graph Coloring*
Kai-Min Chung, Seth Pettie, and Hsin-Hao Su
In Proceedings of the 2014 ACM Symposium on Principles of Distributed Computing (**PODC**), 2014.
Distributed Computing, 30(4):261-280, August 2017

[26] *Physical Randomness Extractors: Generating Random Numbers with Minimal Assumptions*
Kai-Min Chung, Yaoyun Shi, and Xiaodi Wu
Accepted as a *plenary talk* (joint with "Robust Protocols for Securely Expanding Randomness and Distributing Keys Using Untrusted Quantum Devices" by Carl Miller and Yaoyun Shi) at the 17th Conference on Quantum Information Processing (**QIP**), 2014.

[25] *On Extractability (a.k.a. Differing-Inputs) Obfuscation*
Elette Boyle, Kai-Min Chung, and Rafael Pass
In Proceedings of the 11th IACR Theory of Cryptography Conference (**TCC**), 2014.

[24] *4-Round Resettably-Sound Zero Knowledge*
Kai-Min Chung, Rafail Ostrovsky, Rafael Pass, Muthuramakrishnan Venkitasubramaniam, and Ivan Visconti
In Proceedings of the 11th IACR Theory of Cryptography Conference (**TCC**), 2014.

[23] *Interactive Coding, Revisited*
Kai-Min Chung, Rafael Pass, and Sidharth Telang
In Proceedings of the 54th Annual IEEE Symposium on Foundations of Computer Science (**FOCS**), 2013

[22] *Constant-Round Concurrent Zero Knowledge From P-Certificates*
Kai-Min Chung, Huijia Lin, and Rafael Pass
In Proceedings of the 54th Annual IEEE Symposium on Foundations of Computer Science (**FOCS**), 2013

[21] *Simultaneous Resettability from One-Way Functions*
Kai-Min Chung, Rafail Ostrovsky, Rafael Pass, and Ivan Visconti
In Proceedings of the 54th Annual IEEE Symposium on Foundations of Computer Science (**FOCS**), 2013

[20] *Functional Encryption from (Small) Hardware Tokens*
Kai-Min Chung, Jonathan Katz, and Hong-Sheng Zhou
In Proceedings of the 19th Annual International Conference on the Theory and Application of Cryptology and Information Security (**ASIACRYPT**), 2013

[19] *Non-Black-Box Simulation from One-Way Functions And Applications to Resettable Security*
Kai-Min Chung, Rafael Pass, and Karn Seth
In Proceedings of the 45th ACM Symposium on Theory of Computing (**STOC**), 2013.
SIAM Journal on Computing, 45(2):415-458, May 2016

[18] *On the Lattice Smoothing Parameter Problem*
Kai-Min Chung, Daniel Dadush, Feng-Hao Liu, and Chris Peikert
In Proceedings of the 28th Annual IEEE Conference on Computational Complexity (**CCC**), 2013.

[17] *Randomness-Dependent Message Security*
Eleanor Birrell, Kai-Min Chung, Rafael Pass, and Sidharth Telang
In Proceedings of the 10th IACR Theory of Cryptography Conference (**TCC**), 2013.

[16] *Can Theories be Tested? A Cryptographic Treatment of Forecast Testing*
Kai-Min Chung, Edward Lui, and Rafael Pass
In Proceedings of the 4th Innovations in Theoretical Computer Science (**ITCS**), 2013

[15] *On the Power of Nonuniformity in Proofs of Security*
Kai-Min Chung, Huijia Lin, Mohammad Mahmoody, and Rafael Pass
In Proceedings of the 4th Innovations in Theoretical Computer Science (**ITCS**), 2013

[14] *The Knowledge Tightness of Parallel Zero-Knowledge*
Kai-Min Chung, Rafael Pass, and Wei-Lung Dustin Tseng
In Proceedings of the 9th IACR Theory of Cryptography Conference (**TCC**), 2012

[13] *Chernoff-Hoeffding Bounds for Markov Chains: Generalized and Simplified*
Kai-Min Chung, Henry Lam, Zhenming Liu, and Michael Mitzenmacher
In Proceedings of the 29th International Symposium on Theoretical Aspects of Computer Science (**STACS**), 2012

[12] *The Randomness Complexity of Parallel Repetition*
Kai-Min Chung and Rafael Pass
In Proceedings of the 52nd Annual IEEE Symposium on Foundations of Computer Science (**FOCS**), 2011

[11] *Memory Delegation*
Kai-Min Chung, Yael Tauman Kalai, Feng-Hao Liu, and Ran Raz
In Proceedings of the 31st Annual Cryptology Conference (**CRYPTO**), 2011

[10] *Efficient Secure Two-Party Exponentiation*
Ching-Hua Yu, Sherman S.M. Chow, Kai-Min Chung, and Feng-Hao Liu

In Proceedings of the Cryptographer's Track at the RSA Conference (**CT-RSA**), 2011

[9] *Improved Delegation of Computation Using Fully Homomorphic Encryption*
Kai-Min Chung, Yael Tauman Kalai, and Salil P. Vadhan
In Proceedings of the 30th Annual Cryptology Conference (**CRYPTO**), 2010

[8] *Efficient String-commitment From Weak Bit-commitment*
Kai-Min Chung, Feng-Hao Liu, Chi-Jen Lu, and Bo-Yin Yang
In Proceedings of the 16th Annual International Conference on the Theory and Application of Cryptology and Information Security (**ASIACRYPT**), 2010

[7] *Parallel Repetition Theorems for Interactive Arguments*
Kai-Min Chung and Feng-Hao Liu
In Proceedings of the 7th IACR Theory of Cryptography Conference (**TCC**), 2010
Invited to Journal of Cryptology. *Best Student Paper*.

[6] *AMS Without 4-Wise Independence on Product Domains*
Vladimir Braverman, Kai-Min Chung, Zhenming Liu, Michael Mitzenmacher, and Rafail Ostrovsky
In Proceedings of the 27th International Symposium on Theoretical Aspects of Computer Science (**STACS**), 2010

[5] *Tight Bounds for Hashing Block Sources*
Kai-Min Chung and Salil Vadhan
In Proceedings of Approximation, Randomization and Combinatorial Optimization. Algorithms and Techniques, 12th International Workshop, RANDOM 2008 (**RANDOM**), 2008

[4] *S-t Connectivity on Digraphs with a Known Stationary Distribution*
Kai-Min Chung, Omer Reingold, and Salil Vadhan
In Proceedings of the 22nd Annual IEEE Conference on Computational Complexity (**CCC**), 2007
ACM Transactions on Algorithms, 7(3):30, 2011

[3] *An Optimal Algorithm for Maximum-Density Segment Problem*
Kai-Min Chung and Hsueh-I Lu
In Proceedings of European Symposium on Algorithms (**ESA**), 2003
SIAM Journal on Computing, 34(2):373-387, 2004

[2] *Decomposition Methods for Linear Support Vector Machines, Neural Computation*
Kai-Min Chung, Wei-Chun Kao, Chia-Liang Sun, and Chih-Jen Lin
In Proceedings of International Conference on Acoustics, Speech, and Signal Processing (**ICASSP**), 2003.
Neural Computation, 16:1689-1704, 2004.

[1] *Radius Margin Bounds for Support Vector Machines with RBF Kernel*
Kai-Min Chung, Wei-Chun Kao, Chia-Liang Sun, Li Lun Wang, and Chih-Jen Lin
In Proceedings of International Conference on Neural Information Processing (**ICONIP**), 2002
Neural Computation, 15:2643-2681, 2003.

JOURNAL PUBLICATIONS

[17] *Online TSP and Online Dial-a-ride with Predictions*
Hsiao-Yu Hu, Hao-Ting Wei, Meng-Hsi Li, Kai-Min Chung, Chung-Shou Liao
INFORMS Journal on Computing (IJOC), 38(1): 189–206, 2026.

[16] *An Automata-Based Framework for Verification and Bug Hunting in Quantum Circuits*
Yu-Fang Chen, Kai-Min Chung, Ondřej Lengál, Jyun-Ao Lin, Wei-Lun Tsai, Di-De Yen
Communications of the ACM, 68(6): 85–93, 2025.

[15] *On the Need for Large Quantum Depth*
Nai-Hui Chia, Kai-Min Chung, and Ching-Yi Lai
The Journal of the ACM (JACM), 70(1), February 2023

[14] *Foundations of Differentially Oblivious Algorithms*
T-H. Hubert Chan, Kai-Min Chung, Bruce Maggs, and Elaine Shi
The Journal of the ACM (JACM), 69(4), August 2022, Featured Article

[13] *Cryptography with Disposable Backdoors*
Kai-Min Chung, Marios Georgiou, Ching-Yi Lai, and Vassilis Zikas
Cryptography, 3(3): 22, September 2019

[12] *Quantum encryption and generalized Shannon impossibility*
Ching-Yi Lai and Kai-Min Chung
Designs, Codes and Cryptography, 87(9), 1961-1972, January 2019

[11] *On Statistically-Secure Quantum Homomorphic Encryption*
Ching-Yi Lai and Kai-Min Chung
Quantum Information and Computation, 18(9-10): 785-794, August 2018

[10] *Space-efficient classical and quantum algorithms for the shortest vector problem*
Yanlin Chen, Kai-Min Chung,and Ching-Yi Lai
Quantum Information and Computation,18(3 & 4): 283-305,March 2018

[9] *On the Impossibility of Cryptography with Tamperable Randomness*
Per Austrin, Kai-Min Chung, Mohammad Mahmoody, Rafael Pass, and Karn Seth
Algorithmica, 79(4):1052-1101, December 2017

[8] *Distributed algorithms for the Lovász local lemma and graph coloring*
Kai-Min Chung, Seth Pettie, and Hsin-Hao Su
Distributed Computing, 30(4):261-280, August 2017

[7] *Non-Black-Box Simulation from One-Way Functions And Applications to Resettable Security*
Kai-Min Chung, Rafael Pass, and Karn Seth
SIAM Journal on Computing, 45(2):415-458, May 2016

[6] *Guest column: parallel repetition theorems for interactive arguments.*
Kai-Min Chung and Rafael Pass
SIGACT News, 44(1): 50-69, 2013

[5] *Why Simple Hash Functions Work: Exploiting the Entropy in a Data Stream.*
Kai-Min Chung, Michael Mitzenmacher, and Salil P. Vadhan
Theory of Computing, 9: 897-945, 2013

[4] *S-T Connectivity on Digraphs with a Known Stationary Distribution*
Kai-Min Chung, Omer Reingold, and Salil Vadhan
ACM Transactions on Algorithms, 7(3):30, 2011

[3] *Decomposition Methods for Linear Support Vector Machines*
Kai-Min Chung, Wei-Chun Kao, Chia-Liang Sun, and Chih-Jen Lin
Neural Computation, volume 16, number 8, pages 1689-1704, August 2004

[2] *An Optimal Algorithm for Maximum-Density Segment Problem*
Kai-Min Chung and Hsueh-I Lu
SIAM Journal on Computing, 34(2):373-387, 2004

[1] *Radius Margin Bounds for Support Vector Machines with RBF Kernel*
Kai-Min Chung, Wei-Chun Kao, Chia-Liang Sun, Li Lun Wang, and Chih-Jen Lin
Neural Computation, 15: 2643-2681, 2003.

BOOK CHAPTER

[2] *On the Verification of Quantum Circuits (Research Challenges and Opportunities)*
Parosh Aziz Abdulla, Yo-Ga Chen, Yu-Fang Chen, Kai-Min Chung, Lukáš Holík, Ondřej Lengál, Jyun-Ao Lin, Fang-Yi Lo, Wei-Lun Tsai
Principles of Formal Quantitative Analysis, pp. 320–341, 2025

[1] *When Simple Hash Functions Suffice*
Kai-Min Chung and Michael Mitzenmacher and Salil Vadhan
Beyond the Worst-Case Analysis of Algorithms, Chapter 26, 2020

MANUSCRIPTS

[4] *Leakage Chain Rule and Superdense Coding*
Yi-Hsiu Chen, Kai-Min Chung, Ching-Yi Lai, Xiaodi Wu
Manuscript, 2017

[3] *Multi-Source Randomness Extractors Against Quantum Side Information, and their Applications*
Kai-Min Chung, Xin Li, and Xiaodi Wu
Manuscript, 2014

[2] *A Simple ORAM*
Kai-Min Chung and Rafael Pass
Manuscript, 2014

[1] *Unprovable Security of Two-Message Zero-Knowledge*
Kai-Min Chung, Edward Lui, Mohammad Mahmoody, and Rafael Pass
Manuscript, 2013

PATENTS

Rafael Pass, Elette Boyle, and Kai-Min Chung. 2014. Oblivious Parallel Random Access Machine System and Methods.
U.S. Patent Application No. 15/329,730, filed July 31, 2015. Patent issued date:April 2, 2019, Patent No. 10248324

Yaoyun Shi, Kai-Min Chung, and Xiaodi Wu. 2014. Extraction of Random Numbers from Physical Systems.

U.S. Provisional Patent Application No. 61/927,472, filed January 14, 2014. Patent issued date: October 18, 2016, Patent No. 9471280

RESEARCH ADVISING

Postdoctoral Fellows

Jyun-Jie Liao 廖俊杰 May. 2026-Present

- Ph.D., Computer Science, Cornell University, Ithaca, New York, USA
- Research on Randomness in Computation, Computational Complexity, Combinatorics, Cryptography

Tsun-Ming Cheung 張峻銘(co-advised with Prof. Meng-Tsung Tsai) Aug. 2025-Aug. 2026

- Ph.D., Computer Science, McGill University, Montreal, Canada
- Currently an Assistant Professor in the Department of Computer Science, National Tsing Hua University.
- Research on theoretical computer science and discrete mathematics, including communication complexity, streaming algorithms, and quantum computation.

Shih-Han Hung 洪士涵 Nov. 2023-Mar. 2024

- Ph.D., Computer Science, University of Maryland, College Park, USA
- Currently an Assistant Professor in the Department of Electrical Engineering, National Taiwan University.
- Research on Quantum Information Science

Chia-Liang Sun 孫嘉梁 Aug. 2021-Present

- Ph.D., Mathematics, University of Texas at Austin, USA
- Research on Mathematics and Cryptography

Jyun-Ao Lin 林濬璈 Oct. 2020-Jan. 2024

- Ph.D., Mathematics, Paris Diderot University 7, France
- Currently an Assistant Professor in the Department of Computer Science and Information Engineering and the Innovation Frontier Institute of Research for Science and Technology, National Taipei University of Technology.
- Research on Mathematics and Cryptography

Gelo Noel Tabia (co-advised with Prof. Yeong-Cherng Liang) Oct. 2018-Oct. 2020

- Ph.D., Department of Physics and Astronomy, University of Waterloo, Canada
- Currently a Senior Research Scientist at the Quantum Computing Research Center, Hon Hai Research Institute.
- Research on Quantum Cryptography

Han-Hsuan Lin 林瀚仝 Oct. 2016-Nov. 2016

- Ph.D., Physics, Massachusetts Institute of Technology
- Currently an Associate Professor in the Department of Computer Science, National Tsing Hua University.

- Research on Quantum Information

Ching-Yi Lai 賴青沂 Sep. 2015-Jul. 2018

- Ph.D., Electrical Engineering, University of Southern California, Los Angeles
- Currently a Professor in the Institute of Communications Engineering, National Yang Ming Chiao Tung University.
- Research on Quantum Information Theory and Quantum Cryptography

Yu-Chi Chen 陳昱圻 Jan. 2014-Jul. 2017

- Ph.D., Computer Science, National Chung Hsing University
- Research on Cryptography
- Currently a Professor in the Department of Computer Science and Information Engineering, National Taipei University of Technology.

Research Assistants

Yu-Hxiang Chen 陳昱翔 Jul. 2026-Present

- M.S., Department of Mathematics, University of Bonn
- Research on Quantum Complexity

Tzu-Yi Yang 楊子頤 Oct. 2024-Aug. 2026

- M.S., Department of Mathematics, University of Bonn
- Research on Quantum Complexity

Hsien-En Tzeng 曾顯恩 Aug. 2024-Feb. 2026

- B.S., Department of Computer Science and Information Engineering, National Taiwan University
- Ph.D. student at SOKENDAI
- Research on Cryptography,Quantum Information

Yu-Cheng Lu 呂侑承 Aug. 2023-Mar. 2026

- M.S., Department of Electrical Engineering, National Taiwan University
- Research on Cryptography,Quantum Information

Er-Cheng Tang 唐爾晨 Aug. 2022-Aug. 2023

- M.S., Department of Mathematics, National Taiwan University
- Ph.D. student at the University of Washington
- Research on Cryptography,Quantum Information

Tzu-Hsiang Huang 黃資翔 Jul. 2022-Aug. 2025

- B.S., Department of Computer Science and Information Engineering, National Taiwan University
- Ph.D. student at the University of Illinois Urbana-Champaign
- Research on Cryptography

Jhih-Wei Shih 施智偉 Aug. 2021-Present

- B.S., Department of Electrical Engineering, National Taiwan Normal University

- Research on Algorithms and Computational Complexity

Hsiao-Yu Hu 胡筱郁 Mar. 2021- Aug. 2022

- B.S., Department of Industrial Engineering and Engineering Management, National Tsing Hua University
- Ph.D. student at Northwestern University
- Research on Algorithms

Wei-Hsiang Hung 洪偉翔 Oct. 2020-Present

- B.S., Interdisciplinary Program of Electrical Engineering and Computer Science, National Tsing Hua University.
- Research on Cryptography

Yao-Ching Hsieh 謝耀慶 Jul. 2020-Aug. 2022

- B.S., Computer Science and Information Engineering, National Taiwan University.
- Ph.D. student at the University of Washington
- Research on Cryptography

Yuan-Ho Yao 姚元和 Apr. 2020-Mar. 2021

- M.S., Philosophy, National Yang Min University
- Research on Communication Complexity

Yao-Ting Lin 林耀廷 Jan. 2020-Sep. 2022

- M.S., Department of Physics, National Taiwan University.
- Ph.D. student at the University of California, Santa Barbara
- Research on Cryptography and Quantum Information

Shiuan Fu 傅璿 Dec. 2019-May. 2022

- M.S., Mathematics, National Taiwan University.
- Research on Cryptography, Algorithms, Quantum Information, Computational Complexity

Yu-Hsuan Huang 黃右萱 Jul. 2019-Jul. 2021

- M.S., Department of Computer Science, National Chiao-Tung University
- Ph.D., Leiden University
- Currently a Post-Doctoral Researcher at the Max Planck Institute for Security and Privacy (MPI-SP) and the Ruhr University Bochum (RUB).
- Research on Cryptography and Quantum Information

Yi-Hsin Ma 馬宜訢 Jul. 2019-Apr. 2021

- M.S., Department of Applied Mathematics, National Chiao-Tung University.
- Research on Quantum Information

Yu-Ching Shen 沈于晴 Jun. 2019-Aug. 2023

- M.S., Department of Physics, National Taiwan University.
- Ph.D. student at Rice University

- Research on Cryptography

Yi Lee 李懿 Mar. 2019-Nov. 2020

- M.S., Department of Mathematics, Johns Hopkins University.
- Ph.D. student at University of Maryland
- Research on Cryptography, Quantum Information

Chun-Hsiang Chan 詹鈞翔 Sep. 2018-Jul. 2019

- B.S., Electrical Engineering, National Taiwan University
- Research on Cryptography

Hao-Ting Wei 魏豪廷 Sep. 2018-Mar. 2019

- M.S., Department of Industrial Engineering, National Tsing Hua University.
- Ph.D., Columbia University
- Currently a Quantitative Researcher at Vanguard.
- Research on Algorithms

Hao Chung 鍾豪 Sep. 2019-Feb. 2021

- M.S., Electrical Engineering, National Taiwan University
- Ph.D., Carnegie Mellon University
- Currently a Research Engineer at LayerZero Labs.
- Research on Cryptography and Quantum Information

Mi-Ying Huang 黃米瀅 Jul. 2018- Aug. 2021

- B.S. Student, Department of Electrophysics, National Chiao Tung University
- Ph.D., University of Southern California
- Currently a Postdoctoral Research Fellow at Carnegie Mellon University
- Research in cryptography, complexity theory, and learning theory

Kuan-Yi Ho 何冠誼 Dec. 2017-Aug. 2018

- B.S., Electrical Engineering, National Taiwan University
- Research on Algorithms and Complexity

Chun-Peng Chang 張君鵬 Sep. 2017-Apr. 2018

- Ph.D., Physics, National Tsing Hua University
- Research on Quantum Key Distribution Protocols

Jyun-Jie Liao 廖俊杰 Nov. 2016-Aug. 2018

- B.S., Undergraduate Honors Program of Electrical Engineering and Computer Science, National Chiao Tung University
- Ph.D. at Cornell University
- Research on Computational Complexity and Algorithms

Yin-Hsun Huang 黃胤勛 Nov. 2016-Jul. 2017

- B.S., Electrical Engineering, National Taiwan University
- Research on Cryptography

Chi-Ning Chou 周紀寧 Jun. 2016-Jul. 2017

- Research Fellow at Center of Computational Neuroscience at Flatiron Institute, USA
- B.S., Computer Science, National Taiwan University
- Research on Computational Complexity and Algorithms

Yan-Lin Chen 陳彥霖 Jul. 2016-Jun. 2020

- M.S., Electrical Engineering, National Taiwan University
- Ph.D., University of Amsterdam (CWI and QuSoft)
- Currently a Quantum fellow at the School of Mathematics, University of Edinburgh and at the Quantum Software Lab.
- Research on Quantum Information and Cryptography

Tsung-Hsuan Hung 洪琮眩 Jul. 2015-Jan. 2017

- M.S., Mathematical Modeling and Scientific Computing, National Chiao Tung University
- Research on Cryptography

Wei-Kai Lin 林偉楷 Nov. 2014-Jul. 2016

- Assistant Professor at University of Virginia, USA
- M.S., Electrical Engineering, National Taiwan University
- Research on Cryptography

Graduate Students

Ruo-Pu Xuan Wang 王若樸 Sep. 2026-Present

- M.S. Student, Physics, National Taiwan University

Jun-Yi Dong 董俊毅 Sep. 2024-Present

- M.S. Student, Mathematics, National Taiwan University

Yi-Xuan Lee 李怡萱 Oct. 2023-Dec. 2023

- M.S. Student, Electrical Engineering, National Taiwan University
- Research on Algorithm and Complexity

Tong-Nong Lin 林東農 Aug. 2018-Jul. 2019

- M.S. Student, Electrical Engineering, National Taiwan University
- Research on Algorithm and Complexity

Hsien-Ming Pan 潘賢名 Sep. 2018-Jun. 2020

- M.S. Student, Department of Mathematics, National Tsing Hua University

I-Hung Hsu 徐一弘 Sep. 2017-Jun. 2019

- M.S. Student, Department of Mathematics, National Tsing Hua University
- Research on Algorithm and Complexity

Tsung-Hsuan Hung 洪琮眩 Feb. 2017-Aug. 2018

- Ph.D. student, Computer Science and Information Engineering, National Taiwan University
- Research on Cryptography

Hao Chung (co-advised) 鍾豪 Jul. 2016-Aug. 2018

- M.S., Electrical Engineering, National Taiwan University
- Ph.D., Carnegie Mellon University

- Research on Cryptography and Quantum Information

Chiao-Hsun Wang 王教勛 Sep. 2015-Aug. 2017

- M.S. Student, Physics Department, National Taiwan University
- Research on Quantum Cryptography

Yan-Lin Chen (co-advised) 陳彥霖 May 2014-Jun. 2016

- M.S. Student, Electrical Engineering, National Taiwan University
- Research on Quantum Information and Cryptography

Kai-Bin Huang (co-advised short-term) 黃柏凱 May 2014-Dec. 2014

- Ph.D. student, Computer Science, National Chengchi University
- Research on Cryptography

Undergraduate Students

You-Xuan Wu 吳宥瑄 Sep. 2024-Feb. 2025

- Department of Electrical Engineering, National Taiwan University

Tzu-Hsiang Huang 黃資翔 Apr. 2022-Jun. 2022

- Department of Computer Science and Information Engineering, National Taiwan University
- Research on Cryptography

Hsi Tai 戴晞 Jul. 2020-Dec. 2020

- Computer Science, University of Michigan
- Research on Cryptography

Tai-Ning Liao 廖泰甯 Sep. 2018-Jan. 2020

- Department of Electrical Engineering, National Taiwan University

Chun-Chi Wu 吳鈞季 Sep. 2018-Feb. 2019

- Department of Electrical Engineering, National Taiwan University

Tun-Yi Chang 張惇頤 Feb. 2016-Jul. 2017

- Department of Physics, National Taiwan University

Kuan-Yi Ho 何冠誼 Jul. 2016-Jul. 2017

- Electrical Engineering, National Taiwan University
- Research on Algorithm and Complexity

Summer Internship

Ruo-Pu Wang 王若樸 Jul.2026-Aug.2026

- M.S. Student, Physics , National Taiwan University

Cheng-Hsi Tsai 蔡承希 Jul.2026-Aug.2026

- B.S. Student, Electrical Engineering, National Cheng Kung University

Kao-Chuan Liang 梁高銓 Jul.2025-Aug.2025

- B.S. Student, Computer Science , National Tsing Hua University

Ming-Hsien Tsai 蔡名峴 Jul.2025-Aug.2025

- M.S. Student, Electrical Engineering, National Taiwan University

Tzu-Chien Hsu 許子謙 Jul.2025-Aug.2025

- B.S. Student, Electrical engineering, National Taiwan University

Ting Jia Huang 黃梃家 Jul.2025-Aug.2025

- B.S. Student, Computer Science & Information Engineering, National Taiwan University

Teng-Hung Hsiao 蕭登鴻 Jul.2025-Aug.2025

- B.S. Student, Computer Science, National Tsing Hua University

Bo-Wei Lin 林伯蔚 Jul.2024-Aug.2024

- B.S. Student, Computer Science , National Yang Ming Chiao Tung University

Chin-Cheng Liu 劉金丞 Jul.2024-Aug.2024

- B.S. Student, Computer Science , National Yang Ming Chiao Tung University

Jun-Yi Dong 董俊毅 Jul.2024-Aug.2024

- B.S. Student, Mathematics , National Tsing Hua University

Wei-Hsiang Kang 康瑋翔 Jul.2024-Aug.2024

- B.S. Student, Management Information Systems , National Chengchi University

You-Xuan Wu 吳宥瑄 Jul.2024-Aug.2024

- B.S. Student, Electronic Engineering, National Taiwan University

Hsien-En Tzeng 曾顯恩 Jul.2023-Aug.2023

- B.S. Student, Computer Science & Information Engineering, National Taiwan University

Kuan-Hao Chiao 喬冠豪 Jul.2023-Aug.2023

- B.S. Student, Electrical Engineering, National Taiwan University

Keng-Yu Chen 陳耕宇 Jul.2023-Aug.2023

- B.S. Student, Electrical Engineering, National Taiwan University

Chi-Ning Chou 周紀寧 Jul.2015-Aug.2015

- B.S. Student, Computer Science, National Taiwan University

VISITORS HOSTED

Short Term Visitors

Nai-Hui Chia(Rice University, USA)	Nov. 11-20, 2026
Srijita Kundu (Hon Hai Research Institute, Quantum Computing Research Center)	Nov. 4, 2026
Wei-Kai Lin (University of Virginia, USA)	Oct. 6, 2026
Yu-Long Chen (KU Leuven, Belgium)	Oct. 2-8, 2026
Hsien-En Tzeng (SOKENDAI, Japan)	Sep. 15-16, 2026
Yu-Ching Shen (Rice University, USA)	Jun.29-Jul. 5, 2026
Yan-Lin Chen (Joint Center for Quantum Information and Computer Science, USA)	Jun.22-26, 2026
Alper Çakan (Carnegie Mellon University, USA)	May. 29-Jun. 16, 2026
Hung-Wei Tseng (University of California, Riverside, USA)	May. 18-Jun. 10, 2026

ETHAN (YI) LEE (University of Maryland, USA) May. 13-Jul. 27, 2026
Chia-Ying Lin (Rice University, USA) Apr. 20-Aug. 16, 2026
Tomoyuki Morimae (Kyoto University, Japan) Apr. 10-18, 2026
Hao Chung (LayerZero Labs, Canada) Mar. 16-20, 2026
Marvin Beckmann (Technical University of Denmark, Denmark) Mar. 12-13, 2026
Danny Z. Chen (University of Notre Dame, USA) Mar. 1-Apr. 30, 2026
Tomoyuki Morimae (Kyoto University, Japan) Jan. 8-14, 2026
Shogo Yamada (Kyoto University, Japan) Jan. 7-22, 2026
Tzu-Hsiang Huang (University of Illinois Urbana-Champaign, USA) Jan. 5-16, 2026
Chi-Ning Chou (Flatiron Institute, USA) Jan. 5 -Feb. 1, 2026
Er-Cheng Tang (University of Washington, USA) Dec. 22, 2025-Jan. 9, 2026
Wei-Kai Lin (University of Virginia, USA) Dec. 22-24, 2025 & Jan. 2-6, 2026
Mi-Ying Huang (University of Southern California, USA) Dec. 20, 2025-Jan. 20, 2026
Taiga Hiroka (Hon Hai Research Institute, Quantum Computing Research Center) Dec. 18-22, 2025
Ting-Wei Hsieh (University of Washington, USA) Dec. 17, 2025-Jan. 20, 2026
Chia-Hsuan Huang (Theoretical Physics, Caltech, USA) Dec. 17-31, 2025
Yan-Lin Chen (QuICS, the University of Maryland, USA) Dec. 15-26, 2025
Tomoyuki Morimae (Kyoto University, Japan) Dec. 15-22, 2025
Yao-Ting Lin (UC Santa Barbara, USA) Dec. 10-29, 2025
Salil Vadhan (Harvard University, USA) Dec. 9-11, 2025
Danny Chen (University of Notre Dame, USA) Dec. 6-7, 11, 2025
Yossi Azar (Tel Aviv University, Israel) Dec. 5-7, 2025
Mohammad Mahmoody (University of Virginia, USA) Dec. 2-11, 2025
Hakop Pashayan (Hon Hai Research Institute, Quantum Computing Research Center) Nov. 24-Nov. 27, 2025
Masahito Hayashi (Nagoya University, Japan) Jul. 30-Aug. 2, 2025
David Cui (Massachusetts Institute of Technology, USA) Jul. 10-Aug. 4, 2025
Yan-Lin Chen (Algorithms and Complexity, Netherlands) Jun. 30- Jul. 4, 2025
Amin Shiraz Gilani (University of Maryland, USA) Jun. 29- Jul.13, 2025
Andrej Bogdanov (University of Ottawa, Canada) Jun. 24-27, 2025
Yan-Lin Chen (Algorithms and Complexity, Netherlands) Jun. 2-7, 2025
Yao-Ting Lin (UC Santa Barbara, USA) Jun. 2-6, 2025
Nai-Hui Chia (Rice University, USA) May 26- Jun. 19, 2025
Shin Sun (Okinawa Institute of Science and Technology Graduate University, Japan) Apr. 30- May 14, 2025
Tomoyuki Morimae (Kyoto University,Japan) Mar. 25-31, 2025
Shota Yamada (National Institute of Advanced Industrial Science and Technology, Japan) Mar. 19-28, 2025
Akshima (NYU Shanghai, China) Feb. 28- Apr. 1, 2025
Chi-Ning Chou(Flatiron Institute, USA) Feb. 5-13, 2025
Yun Lu (University of Victoria, Canada) Jan. 1-24, 2025
Si-Yao Guo (NYU Shanghai, China) Jan. 1- Dec. 12, 2025
Yu-Hsuan Huang (Centrum Wiskunde & Informatica, Netherlands) Dec. 27, 2024-Jan. 1, 2025
Chin Ho Lee (North Carolina State University, USA) Dec. 17-23, 2024
Yao-Ching Hsieh (University of Washington, USA) Dec. 13, 2024-Jan. 9, 2025
Er-Cheng Tang (University of Washington, USA) Dec. 6-20, 2024
Yan-Lin Chen (Algorithms and Complexity, Netherlands) Dec. 3, 2024-Jan. 11, 2025

Mi-Ying Huang(University of Southern California, USA)	Nov. 18- Dec. 28, 2024
Hao Chung (Carnegie Mellon University, USA)	Sep. 18- Oct. 15, 2024
Yan-Lin Chen (Algorithms and Complexity, Netherlands)	Aug. 29- Sep. 3, 2024
Aditya Gulati (University of California, Santa Barbara, USA)	Aug. 19- Sep. 14, 2024
Jyun-Jie Liao (University of California San Diego, USA)	Aug. 1-31, 2024
Si-Yao Guo (NYU Shanghai, China)	Aug. 1-31, 2024
Nai-Hui Chia (Rice University, USA)	Jul. 8-24, 2024
Aditya Gulati (University of California, Santa Barbara, USA)	Jun. 24-Jul. 19, 2024
Pei-San Huang (University of Houston, USA)	Jun. 19-Jul. 25, 2024
David Junzi Wu (The University of Texas at Austin, USA)	Jun. 19-23, 2024
Yao-Ching Hsieh (University of Washington, USA)	Jun. 1-26, 2024
Hao Chung (Carnegie Mellon University, USA)	Feb. 22-Mar. 9, 2024
Tomoyuki Morimae (Kyoto University, Japan)	Feb. 17-21, 2024
Yu-Hsuan Huang (Centrum Wiskunde & Informatica, Netherlands)	Jan. 21-27, 2024
Yu-Ching Shen (Rice University, USA)	Jan. 20-25, 2024
Zheng-Yi Han (Rice University, USA)	Jan. 20-25, 2024
Wan-Bing Zhao (Rice University, USA)	Jan. 20-25, 2024
Shota Yamada (AIST, Japan)	Jan. 10-Feb. 8, 2024
Chi-Ning Chou (Flatiron Institute, USA)	Jan. 10-15, 2024
Yi-Xin Shen (King's College London, UK)	Jan. 8-12, 2024
Er-Cheng Tang (University of Washington, USA)	Dec. 19, 2023-Jan. 14, 2024
Yan-Lin Chen (Algorithms and Complexity, Netherlands)	Dec. 16, 2023-Jan. 20, 2024
Yun Lu (University of Victoria, Canada)	Dec. 11-22, 2023
Yao-Ting Lin (UC Santa Barbara, USA)	Dec. 9, 2023-Jan. 5, 2024
Hsiao-Yu Hu (Northwestern University, USA)	Dec. 5-30, 2023
Noam Mazor (Cornell Tech, USA)	Dec. 4-8, 2023
Russell W. F. Lai (Aalto University, Finland)	Dec. 4-8, 2023
Giulio Malavolta (Bocconi University, Italy)	Dec. 3-7, 2023
Ethan Yi Lee (University of Maryland, USA)	Nov. 29-Dec. 8, 2023
Mi-Ying Huang (University of Southern California, USA)	Nov. 28-Dec. 14, 2023
Zvika Brakerski (Weizmann Institute of Science, Israel)	Nov. 28-Dec. 3, 2023
Brian Andrew LaMacchia (Farcaster Consulting Group, USA)	Nov. 27-Dec. 5, 2023
Xin-Yu Mao (University of Southern California, USA)	Nov. 27-Dec. 4, 2023
Iftach Haitner (Tel Aviv University, Israel)	Nov. 27-Dec. 4, 2023
Tal Malkin (Columbia University, USA)	Nov. 25-Dec. 4, 2023
Jia-Peng Zhang (University of Southern California, USA)	Nov. 25-Dec. 2, 2023
Hsin-Hao Su (Boston College, USA)	Nov. 15-17, 2023
Luca Trevisan (Bocconi University, Italy)	Aug. 16-24, 2023
Jyun-Jie Liao (Cornell University, USA)	Jul. 24-Aug. 3, 2023
Ansis Rosmanis (Nagoya University, Japan)	Jul. 10-14, 2023
Han-Hsuan Lin (National Tsing Hua University, Taiwan)	Jul. 1-Aug. 31, 2023
Si-Yao Guo (NYU Shanghai, China)	Jul. 1-31, 2023
Yao-Ting Lin (UC Santa Barbara, USA)	Jun. 26-Jul. 24, 2023
Mi-Ying Huang (University of Southern California, USA)	Jun. 13-Aug. 17, 2023
Yao-Ching, Hsieh (University of Washington, USA)	Jun. 12-Jul. 18, 2023
Ethan Yi Lee (University of Maryland, USA)	Jun. 12-Aug. 18, 2023
Eli Goldin (New York University, USA)	Jun. 3-Jul. 31, 2023

Taiga Hiroka (Kyoto University, Japan)	May 22-26, 2023
Minki Hhan (Korea Institute For Advanced Study, Korea)	May 18-27, 2023
Takashi Yamakawa (NTT Social Informatics Laboratories, Japan)	May 15-25, 2023
Tomoyuki Morimae (Kyoto University, Japan)	May 13-21, 2023
Shih-Han Hung (University of Texas at Austin, USA)	Apr. 11-15, 2023
Luca Trevisan (Bocconi University, Italy)	Jan. 5-14, 2023
Chi-Ning Chou (Carnegie Mellon University, USA)	Dec. 30, 2022-Jan. 19, 2023
Hao Chung (Carnegie Mellon University, USA)	Dec. 24, 2022-Jan. 15, 2023
Mi-Ying Huang (University of Southern California)	Dec. 22, 2022-Jan. 4, 2023
Andreas H‘ijlsing (Eindhoven University of Technology, Netherlands)	Dec. 10-15, 2022
Yingkai Ouyang (National University of Singapore, Singapore)	Dec. 10-14, 2022
Christopher Brzuska (Aalto University, Finland)	Dec. 10-18, 2022
Christoph Egger (Institut de Recherche en Informatique Fondamentale, France)	Dec. 10-17, 2022
Dominique Unruh (University of Tartu, Estonia)	Dec. 1-19, 2022
Li Chen (Georgia Institute of Technology, USA)	Sep. 10-25, 2022
Omri Shmueli (Tel Aviv University, Israel)	Sep. 1-10, 2022
Nai-Hui Chia (Indiana University Bloomington, USA)	Jul. 6-8, 2022
Mi-Ying Huang (University of Southern California, USA)	Jul. 2-19, 2022
Kazuo Iwama (RIMS, Kyoto University, Japan)	Jun. 23-26, 2022
Hao Chung (Carnegie Mellon University, USA)	Dec. 31, 2021-Jan. 22, 2022
Yan-Lin Chen (CWI and QuSoft, Netherlands)	Dec. 17, 2021-Jan. 15, 2022
Yan-Lin Chen (CWI and QuSoft, Netherlands)	Dec. 21, 2020-Jan. 15, 2021
Liang Yeong-Cherng (NCKU, Taiwan)	July. 8-15, 2020
Jyun-Ao Lin(Xiamen University Malaysia,Malaysia)	Feb. 14-Mar.22, 2020
Hoeteck Wee (École normale supérieure, France)	Jan. 1-7, 2020
Hubert Chan (The University of Hong Kong, China)	Dec. 23, 2019-Jan. 3, 2020
Elaine Shi (Cornell University, USA)	Dec. 17, 2019-Jan. 10, 2020
Min-Hsiu Hsieh (University of Technology Sydney, Australia)	Nov. 29, 2019-Jan. 25, 2020
Yuyi Wang (ETH Zürich, Switzerland)	Oct. 28-Nov. 7, 2019
Takashi Yamakawa (NTT, Japan)	Oct. 6-Nov. 5, 2019
Han-Hsuan Lin (UTCS,USA)	Aug. 19-Sep. 4, 2019
Hong-Sheng Zhou (Virginia Commonwealth University,USA)	Jul. 2-4, 2019
Penghui Yao (Nanjing University, China)	Feb. 17-28, 2019
Shota Yamada (National Institute of Advanced Industrial Science and Technology)	Apr. 14-21, 2019
Angela Capel Cuevas (ICMAT-Institute of Mathematical Sciences, Spain)	Jun. 25-Sep. 14, 2018
Chen-Fu Chiang (SUNY Polytechnic Institute, USA)	Jun. 6, 2018
Somitra Kumar Sanadhya (IIT Ropar, India)	May 15-Jul. 19, 2018
Amit Kumar Chauhan (IIT Ropar, India)	May 15-Jul. 29, 2018
Min-Hsiu Hsieh (University of Technology Sydney, Australia)	Apr. 2, 2018
Yingkai Ouyang (National University of Singapore, Singapore)	Mar. 14-22, 2018
Zvika Brakerski (Weizmann Institute of Science, Israel)	Feb. 15-24, 2018
Elette Boyle (IDC Herzliya, Israel)	Feb. 15-24, 2018
Yicong Zheng (National University of Singapore, Singapore)	Dec. 3-9, 2017
Danny Chen (University of Notre Dame, USA)	Nov. 26-Dec. 4, 2017
Kharchenko Natalia (Universite Pierre et Marie Curie, France)	Oct. 1-Nov. 30, 2017
Masahito Hayashi (Nagoya University, Japan)	Aug. 27-Sep. 1, 2017
Hao-Chung Cheng (University of Technology Sydney, Australia)	Jul. 10-14, 2017

Yicong Zheng (National University of Singapore, Singapore)	May 7-14, 2017
Xiongfeng Ma (TsingHua University, Beijing, China)	Feb. 13-19, 2017
Min-Hsiu Hsieh (University of Technology Sydney, Australia)	Jan. 25-Feb. 16, 2017
Vassilis Zikas (Rensselaer Polytechnic Institute, New York, USA)	Jan. 5-13, 2017
Luca Trevisan (University of California, Berkeley, USA)	Jan. 3-9, 2017
Cedric Lin (University of Maryland, USA)	Dec. 25, 2016-Jan. 6, 2017
Prabhanjan Ananth (University of California, Los Angeles, USA)	Dec. 5-16, 2016
Marios Georgiou (City University of New York, USA)	Oct. 31-Nov. 6, 2016
Ilan Komargodski (Weizmann Institute of Science, Israel)	Oct. 1-15, 2016
Mark Bun (Harvard University, USA)	May 16-25, 2016
Yuichi Yoshida (National Institute of Informatics, Japan)	May 16-18, 2016
Georgios Piliouras (Singapore University of Technology and Design, Singapore)	May 15-18, 2016
Anthony Man-Cho, So (The Chinese University of Hong Kong, Hong Kong)	Mar. 25-28, 2016
Shengyu Zhang (The Chinese University of Hong Kong, Hong Kong)	Mar. 25-28, 2016
Xin Han (Dalian University of Technology, China)	May 13-17, 2016
Ran Cohen (Bar-Ilan University, Israel)	May 01-10, 2016
Mark Simkin (Saarland University, Germany)	Mar. 01-10, 2016
Yuval Ishai (Technion, Israel and UCLA, USA)	Feb. 29-Mar. 10, 2016
Hsin-Hao Su (Massachusetts Institute of Technology, USA)	Dec. 23-26, 2015
Meng-Tsung Tsai (Rutgers University, USA)	Dec. 17-24, 2015
Nai-Hui, Chia (Penn State University, USA)	Dec. 16-23, 2015
Christopher Williamson (Chinese University of Hong Kong)	Dec. 6-8, 2015
Luca Trevisan (University of California, Berkeley, USA)	Dec. 5-15, 2015
Gang Xu (Beijing University of Posts and Telecommunications, China)	Dec. 1-9, 2015
Hao-Chung Cheng (University of Technology Sydney, Australia)	Nov. 27-Dec. 2, 2015
Thomas Steinke (Harvard University, USA)	Aug. 22-27, 2015
Siyao Guo (CUHK, Hong Kong)	Apr. 20-25, 2015
Yeong-Cherng Liang (NCKU, Taiwan)	Apr. 13-15, 2015
Muthuramakrishnan Venkitasubramaniam (Rochester University, USA)	Mar. 8-14, 2015
Lior Seeman (Cornell University, USA)	Dec. 18-23, 2014
Yitong Yin (Nanjing University, China)	Dec. 15-25, 2014
Fang Song (University of Waterloo, Canada)	Dec. 6-13, 2014
Arno Mittelbach (CASED, Germany)	Dec. 3-6, 2014
Christina Brzuska (Microsoft Research Cambridge, UK)	Dec. 3-6, 2014
Andrej Bogdanov (CUHK, Hong Kong)	Nov. 18-23, 2014
Chung-Chih Li (Illinois State University, USA)	Jul. 9, 2014
Hsin-Hao Su (University of Michigan, USA)	Jan. 25-28, 2014
Sze-Ming Sherman Chow (CUHK, Hong Kong)	Jan. 9-15, 2014
David Xiao (CNRS, France)	Nov. 20-23, 2013

TALKS

Constant-Rate Certified Deletion

Physics Colloquium, Department of Physics, National Cheng Kung University,Taiwan 10/16/2026

Constant-Rate Certified Deletion

Physics Colloquium, Department of Physics, National Cheng Kung University,Taiwan 10/16/2026

Complexity theory for quantum-input decision problems and computational hardness in quantum cryptography

SG Crypto Workshop, National University of Singapore, Singapore 1/5/2026

Complexity Theory for Quantum Promise Problems

YITP Workshop Kyoto Quantum Crypto 2, Kyoto University, Japan 10/22/2025
AS Conference, Academia Sinica, Taiwan 07/03/2025

On the Impossibility of General Parallel Fast-forwarding of Hamiltonian Simulation
Department of Electrical Engineering, National Taiwan University, Taiwan 02/26/2024
Department of Computer Science & Information Engineering,
National Taiwan University, Taiwan 12/22/2023
National Center for Theoretical Sciences, National Cheng Kung University, Taiwan 05/22/2023
Computer and Information Network Center, National Chung Hsing University, Taiwan 07/04/2023

Post-Quantum Cryptography: The Key to Resisting Quantum Attack (Popular Science Talk)
Aerospace Technology Research and Development Center,
Chung Yuan Christian University, Taiwan 09/07/2022

Theoretical Aspects of Post-Quantum Cryptography
Cybersecurity Center of Excellence (CCOE), Taiwan 07/08/2022

Potential and Limit of Quantum Computing (Popular Science Talk)
Post-quantum Cryptography Forum, Taiwan 01/14/2022

A personal view on quantum computation and cryptography and an interactive discussion
Institute of Statistical Science, Academia Sinica, Taiwan 10/18/2021

Compressed Oracle as a Quantum Lazy Sampling Technique
Workshop on Quantum Techniques for Provable Security (QUIQUES), Croatia (Virtual) 10/17/2021

Tight Quantum Time-Space Tradeoffs for Function Inversion
International Conference on the 16th TQC 2021, Latvia (Virtual) 07/07/2021
The Second Kyoto Workshop on Quantum Information, Computation, and Foundation
(QICF21), Japan (Virtual) 09/14/2021

On the Power of Hybrid Classical and Low-depth Quantum Computation
Institute of Network Engineering Seminar, NYCU, Taiwan 05/05/2021
Department of Computer Science Seminar, NTHU, Taiwan 04/28/2021
Joint CQSE-NCTS-CASTS-CTP Seminar, NTU, Taiwan 04/16/2021
Workshop on Quantum Science and Technology (QST), Taiwan 08/20/2020

How well can a classical client delegate quantum computation?
Pengcheng Lab Quantum Computing Research Center, China 07/17/2020
Centre for Quantum Software and Information, UTS, Australia 06/02/2020

Quantum Cryptography and Quantum Complexity
Quantum Information Science (QIS) and Mathematics, Taiwan 10/17/2020

Meeting the Quantum Era — A Brief Talk on the Potential and Limits of Quantum Computing (Popular Science Talk)
Institute of Information Science, Academia Sinica, Taiwan 10/26/2019

TCS, Crypto and Quantum
Institute of Information Science, Academia Sinica, Taiwan 11/29/2019

On the Hardness of Massively Parallel Computation
Lower Bounds in Cryptography, Bertinoro, Italy 07/08/2019
Department of Computer Science, Cornell University, USA 08/01/2019

On the Algorithmic Power of Spiking Neural Networks
AI forum 2019, National Chung Hsing University, Taiwan 04/26/2019

When Schrodinger meets Turing — Cryptography 2.0 in the Quantum Era (Popular Science Talk)
Department of Computer Science and Engineering, Yuan Ze University, Taiwan 03/29/2019
Prospect Talk Series for Popular Science, National Taiwan University, Taiwan 06/15/2018

Privacy Amplification against Active Quantum Adversaries and Quantum-Proof Non-Malleable Extractors
Department of Computer Science, University of Maryland, USA 03/06/2019

Intro to Pseudo-randomness
IISC-IACR School on Cryptology, Indian Institute of Science, Bangalore, India 01/04/2018

Randomness Extraction in the Quantum World
Workshop on The New Theory and Application in Cryptography, Sanya, China 12/14/2017
International Conference on Information Theoretic Security (ICITS) 2017, Hong Kong, China

12/01/2017

Computational Notions of Quantum Min-Entropy
Workshop on Quantum Algorithms and Complexity Theory, CQT, Singapore 02/27/2018
Workshop on Quantum Science and Technology, NCTS, Taipei, Taiwan 09/06/2017

General Randomness Amplification with Non-signaling Security
IIIS, Tsinghua University, Beijing, China 06/02/2017
Department of Computer Science, Cornell University, USA 04/20/2017
CQT CS Talk, Centre for Quantum Technologies, Singapore 02/22/2017
Winter'17 Quantum Day @ Portland, Portland, USA 01/13/2017

True Randomness from Minimal Assumptions
Department of Computer and Electrical Engineering and Computer Science, FAU, USA 03/26/2017
Institute for Interdisciplinary Information Sciences, Beijing, China 12/23/2016
Workshop on Mathematics of Information -Theoretic Cryptography 2016, Singapore 09/29/2016
Trustworthy Quantum Information (TYQI) 2016, Shanghai, China 06/30/2016

Computational Notions of Quantum Entropy
Tsinghua-Cornell Workshop on Security and Cryptography, Beijing, China 12/22/2016
The Quantum-Safe Crypto Workshop 2016, Singapore 10/03/2016

Randomness Extractors beyond the Classical Setting
Shanghai University of Finance and Economics (SUFE), 2016, Shanghai, China 06/18/2016
Workshop on Spectral Graph Theory and Its Applications 2015, Taipei, Taiwan 12/09/2015

Cryptography for Parallel RAM from Indistinguishability Obfuscation
DIMACS/MACS Workshop on Cryptography for the RAM Model of Computation(DIMACS) 2016, Boston, USA 06/09/2016

Toward Cryptography for Modern Parallel Architecture
Asian Association for Algorithms and Computation (AAAC) 2016, Taipei, Taiwan 05/16/2016

No-signalling Secure Physical Randomness Extractors, or Randomness Amplification for Arbitrary Weak Sources
Workshop on Quantum Nonlocality, Causal Structures and Device-independent Quantum Information 2015, Tainan, Taiwan 12/14/2015

Randomness Extraction beyond the Classical World
International Conference on Quantum Cryptography (QCrypt) 2015, Tokyo, Japan 09/29/2015

Randomness Extractors: from Classical to Quantum Worlds
University of Michigan, International Workshop: Trustworthy Quantum Information 06/29/2015

Multi-Source and Network Extractors in the Presence of Quantum Side Information
National Taiwan University, CQSE-CASTS Seminar 05/01/2015
Institute for Quantum Computing, University of Waterloo, Seminar 10/23/2014

Physical Randomness Extractors: Generating Random Numbers with Minimal Assumptions
National Cheng Kung University, Seminar 04/16/2015
Institute of Statistical Science, Academia Sinica, Seminar 05/12/2014
National Taiwan University, CASTS Seminar 05/09/2014
Simons' Institute, Quantum Gathering 04/09/2014

Computation-Trace Indistinguishability Obfuscation and its Applications
Microsoft Research, London 04/07/2015

Tight Parallel Repetition Theorems for Public-Coin Arguments using KL-divergence
Theory of Cryptography Conference (TCC) 2015, Warsaw, Poland 03/25/2015

Statistically-secure ORAM with $\tilde{O}(\log^2 n)$ Overhead
National Cheng Kung University, Tainan, Taiwan 03/06/2015
National Tsing Hua University, Seminar 12/17/2014
ASIACRYPT Conference 2014 12/10/2014
National Chung Hsing University, Seminar 05/16/2014
University of California Santa Barbara, Colloquium 02/18/2014

(Cryptography) Research in Taiwan
International View of the State-of-the-Art of Cryptography and Security and its Use in Practice (VI), joint presentation with Dr. Bo-Yin Yang 12/12/2014

Interactive Coding, Revisited
NYU, Crypto Seminar 12/03/2013
MSR-Silicon Valley Theory, Seminar 08/26/2013
University of Maryland, Crypto Seminar 07/17/2013

On the Lattice Smoothing Parameter Problem
Purdue University Theory Seminar 06/18/2013
CCC'13 06/07/2013

Can Theories be Tested? A Cryptographic Treatment of Forecast Testing
DIMACS Workshop on Current Trends in Cryptology 05/01/2013
Cornell Theory Seminar 04/01/2013

On the (Im)Possibility of Tamper-Resilient Cryptography: Using Fourier Analysis in Computer Viruses

IBM Research Cryptography Seminar	09/17/2012
NYU Cryptography Seminar	09/12/2012

Recent Progress on Parallel Repetition

University of Michigan Theory Seminar	03/11/2013
NYU Theory Seminar	09/13/2012
Academia Sinica IIS Seminar	03/28/2012
University of Connecticut CSE Colloquia	03/12/2012
National Taiwan University	12/30/2011

The Knowledge Tightness of Parallel Zero-Knowledge

TCC'12	03/21/2012

Chernoff-Hoeffding Bounds for Markov Chains: Generalized and Simplified

STACS'12	03/03/2012

The Randomness Complexity of Parallel Repetition

BU Security Seminar	02/28/2012
Penn-State University CSE Seminar	01/19/2012
FOCS'11	10/25/2011
Cornell Theory Seminar	09/26/2011

Memory Delegation

CRYPTO'11	08/15/2011
Harvard Theory of Computation Seminar	04/22/2011

Improved Delegation of Computation Using Fully Homomorphic Encryption

New York Crypto Day	10/14/2010
CRYPTO'10	08/18/2010
Verifiable Computation Workshop, MIT	08/11/2010

Security Amplification via Parallel Repetition

Cornell Cryptography Seminar	03/17/2010
Georgia Tech ARC Colloquium	02/15/2010

Parallel Repetition Theorems for Interactive Arguments

TCC'10	02/09/2010
MIT CIS/Microsoft Seminars	12/11/2009
Brown Theory Lunch	12/08/2009

Tight Bounds for Hashing Block Sources

Harvard Theory of Computation Seminar	11/10/2008
Approx-Random'08	08/25/2008

S-t Connectivity on Digraphs with a Known Stationary Distribution

CCC'07	06/15/2007

An Optimal Algorithm for the Maximum-Density Segment Problem

ESA'03	09/18/2003