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@iis.sinica.edu.tw
http://www.iis.sinica.edu.tw/pages/kmchung/
http://www.iis.sinica.edu.tw/~kmchung/

Current Position

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

Previous Position

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*
- Visiting student at University of California, Berkeley Sep. 2007 – Jun. 2008

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 and Quantum Complexity Theory

Honors and Awards

MOST Outstanding Research Award 2021

Academia Sinica Investigator Award 2021
associated with a five-year 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

IICM K. T. Li Young Researcher Award 2017

FAOS Young Scholar Creative Research Award 2017

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

Simons-Berkeley Research Fellowships in Cryptography 2015

Li Foundation Heritage Prize 2014

Simons Postdoctoral Fellowship 2010

Best Student Paper Award at TCC 2010 2010
for paper "Parallel Repetition Theorems for Interactive Arguments" (with Feng-Hao Liu)

SYNERGISTIC ACTIVITIES

General Chair

- 19th International Conference on the Theory and Practice of Public-Key Cryptography (PKC 2016)

Organizing Committee

- 16th Asian Quantum Information Science Conference (AQIS 2016)

Organizer

- Theory Day in Taiwan 2020, Winter Theory Workshop
- Theory Day in Taiwan 2020, New Year Special
- Theory Day in Taiwan 2019-A, B
- Theory Day in Taiwan 2018, Post X-mas Special
- Theory Day in Taiwan 2017-A, B, C
- Theory Day in Taiwan 2016-A, B

Program Committee

- 54th Annual ACM Symposium on Theory of Computing (STOC 2022)
- 2nd Conference on Information-Theoretic Cryptography (ITC 2021)
- 27th Annual International Conference on The Theory and Application of Cryptology and Information Security (Asiacrypt 2021)
- 27th International Computing and Combinatorics Conference (COCOON 2021)
- 40th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT 2021)
- 18th IACR Theory of Cryptography Conference (TCC 2020)
- Conference on Information-Theoretic Cryptography (ITC 2020)

- 23rd International Conference on the Theory and Practice of Public-Key Cryptography (PKC 2020)
- 17th IACR Theory of Cryptography Conference (TCC 2019)
- 38th Annual International Cryptology Conference (CRYTPO 2019)
- 38th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT 2019)
- 29th International Symposium on Algorithms and Computation (ISAAC 2018)
- 8th International Conference on Quantum Cryptography (QCrypt 2018)
- 21st International Conference on the Theory and Practice of Public-Key Cryptography (PKC 2018)
- 23rd Annual International Conference on the Theory and Application of Cryptology and Information Security (Asiacrypt 2017)
- 15th IACR Theory of Cryptography Conference (TCC2017)
- 32nd Computational Complexity Conference (CCC 2017)
- 14th IACR Theory of Cryptography Conference-B (TCC2016)
- 21st Annual International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT 2015)
- 26th International Symposium on Algorithms and Computation (ISAAC 2015)
- 12th Theory of Cryptography Conference (TCC 2015)
- 11th Theory of Cryptography Conference (TCC 2014)
- 20th Annual International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT 2014)
- 33rd Annual International Cryptology Conference (CRYPTO 2013)

GRANTS

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

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 2018-2023
Funded by Ministry of Science and Technology, Taiwan.
(No: MOST 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)

Short-term Abroad Research Program Jan.-Dec. 2015
Funded by Ministry of Science and Technology, Taiwan.

PATENTS

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

Yaoyun Shi, Kai-Min Chung, 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

CONFERENCE PUBLICATIONS

[58] *On the Compressed-Oracle Technique, and Post-Quantum Security of Proofs of Sequential Work*
Kai-Min Chung, Serge Fehr, Yu-Hsuan Huang, Tai-Ning Liao
to appear in The 40th Annual International Conference on the Theory and Applications of Cryptographic Techniques (**Eurocrypt**), 2021.

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

[56] *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.

[55] *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.

[54] *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.

[53] *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.

[52] *On the Need for Large Quantum Depth*
Nai-Hui Chia, Kai-Min Chung, Ching-Yi Lai
In proceedings of STOC, 2020 (**STOC**), 2020.
Accepted by QIP as a contributed talk, 2020 (**QIP**), 2020..

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

[50] *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.

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

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

[47] *Foundations of Differentially Oblivious Algorithms*
Kai-Min Chung, T-H. Hubert Chan, Bruce Maggs and Elaine Shi
In proceedings of ACM-SIAM Symposium on Discrete Algorithms (**SODA**), 2019.

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

[45] *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.

[44] *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.

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

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

[41] *General Randomness Amplification with Non-signaling Security*
Kai-Min Chung and Yaoyun Shi and Xiaodi Wu
Accepted by QIP as a contributed talk, 2017 (**QIP**), 2017..

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

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

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

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

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

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

[34] *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.

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

[32] *Statistically-secure ORAM with $\tilde{O}(\log^2 n)$ Overhead*
Kai-Min Chung and 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.

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

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

[29] *Physical Randomness Extractors: Generating Random Numbers with Minimal Assumptions*
Kai-Min Chung and 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.

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

[27] *4-Round Resettably-Sound Zero Knowledge*
Kai-Min Chung and Rafail Ostrovsky and Rafael Pass and Muthuramakrishnan Venkitasubramaniam and Ivan Visconti
In proceedings of the 11th IACR Theory of Cryptography Conference (**TCC**), 2014.

[26] *Multi-Source Randomness Extractors Against Quantum Side Information, and their Applications*
Kai-Min Chung and Xin Li and Xiaodi Wu
In proceedings of ECCC 2014 (**ECCC**), 2014

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

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

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

[22] *Why Simple Hash Functions Work: Exploiting the Entropy in a Data Stream*
Kai-Min Chung and Michael Mitzenmacher and Salil P. Vadhan
Theory of Computing, 9(30):897–945, 2013

[21] *Functional Encryption from (Small) Hardware Tokens*
Kai-Min Chung and 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

[20] *Non-Black-Box Simulation from One-Way Functions And Applications to Resettable Security*
Kai-Min Chung and Rafael Pass and Karn Seth
In proceedings of the 45th ACM Symposium on Theory of Computing (**STOC**), 2013.

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

[18] *Parallel Repetition Theorems for Interactive Arguments*
Kai-Min Chung and Rafael Pass
SIGACT News, Complexity Theory Column, Volumn 44 Issue 1, March 2013.

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

[16] *A Cryptographic Treatment of Forecast Testing*
Kai-Min Chung and 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 and Huijia Lin and 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 and 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 and Henry Lam and Zhenming Liu and Michael Mitzenmacher
In proceedings of the 28th 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 and Yael Tauman Kalai and 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 and Sherman S.M. Chow and 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 and 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 and Feng-Hao Liu and 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
Best Student Paper ; invited to Journal of Cryptology.

[6] *AMS Without 4-Wise Independence on Product Domains*
Vladimir Braverman and Kai-Min Chung and Zhenming Liu and Michael Mitzenmacher and Rafail Ostrovsky
In the proceedings of the 26th 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 and 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 and Wei-Chun Kao and 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 and Wei-Chun Kao and Chia-Liang Sun and Li Lun Wang, Chih-Jen Lin
In proceedings of International Conference on Neural Information Processing (**ICONIP**), 2002
Neural Computation, 15:2654-2681, 2003.

JOURNAL PUBLICATIONS

[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
Design, 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*
Ching-Yi Lai and Yanlin Chen and Kai-Min Chung
Quantum Information and Computation,18(3 & 4): 285-306,January 2018

[9] *On the Impossibility of Cryptography with Tamperable Randomness*
Per Austrin and Kai-Min Chung and Mohammad Mahmoody and 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 and 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 and 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 and Omer Reingold and Salil Vadhan
ACM Transactions on Algorithms, 7(3):30, 2011

[3] *Decomposition Methods for Linear Support Vector Machines*
Kai-Min Chung and Wei-Chun Kao and Chia-Liang Sun and Chih-Jen Lin
Neural Computation, volume16, number8, pages1689-1704, 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 and Wei-Chun Kao and Chia-Liang Sun and Li Lun Wang, Chih-Jen Lin
Neural Computation, 15: 2654-2681, 2003.

MANUSCRIPTS

[5] *On the Impossibility of Post-Quantum Black-Box Zero-Knowledge in Constant Rounds*
Nai-Hui Chia, Kai-Min Chung, Qipeng Liu, Takashi Yamakawa
Manuscript, 2021

[4] *Constant-round Blind Classical Verification of Quantum Sampling*
Kai-Min Chung, Yi Lee, Han-Hsuan Lin, Xiaodi Wu
Manuscript, 2020

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

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

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

IN SUBMISSION

[5] *Collusion-Resistant Functional Encryption for RAMs*
Prabhanjan Ananth, Kai-Min Chung, Xiong Fan, Luowen Qian
In Submission, 2021

[4] *On the Concurrent Composition of Quantum Zero-Knowledge*
Prabhanjan Ananth, Kai-Min Chung, Rolando L. La Placa
In Submission, 2021

[3] *A Black-Box Approach to Post-Quantum Zero-Knowledge in Constant Rounds*
Nai-Hui Chia, Kai-Min Chung, Takashi Yamakawa
In Submission, 2021

[2] *Round Efficient Secure Multiparty Quantum Computation with Identifiable Abort*
Bar Alon, Hao Chung, Kai-Min Chung, Mi-Ying Huang, Yi Lee, Yu-Ching Shen
In Submission, 2021

[1] *Game-Theoretic Fairness Meets Multi-Party Protocols: The Case of Leader Election*
Kai-Min Chung, T-H Hubert Chan, Ting Wen, Elaine Shi
In Submission, 2021

BOOK CHAPTER

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

RESEARCH ADVISING

Postdoctoral Fellows

Jyun-Ao Lin Oct. 2020-Present

- Ph.D., Mathematics, Paris Diderot University 7, France
- Research on Mathematics

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

- Ph.D., Department of Physics and Astronomy, University of Waterloo, Canada
- Research on Quantum Cryptography

Ching-Yi Lai Sep. 2015-Jul. 2018

- Ph.D., Electrical Engineering, University of Southern California, Los Angeles
- Research on Quantum Information Theory and Quantum Cryptography
- Now as an assistant professor at Inst. of Comm. Eng., National Chiao Tung University

Yu-Chi Chen Jan. 2014-Jul. 2017

- Ph.D., Computer Science, National Chung Hsing University
- Research on Cryptography
- Now as an assistant professor at Dept. of Comp. Sci. and Engineering, Yuan Ze University

Han-Hsuan Lin Oct. 2016-Nov. 2016

- Ph.D., Physics, Massachusetts Institute of Technology
- Research on Quantum Information
- Now as a postdoc at UT Austin

Research Assistants

Wei-Hsiang Hung Oct. 2020-Present

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

- Research on Cryptography

Yao-Ching Hsieh Jul. 2020-Present

- B.S., Computer Science and Information Engineering, National Taiwan University.
- Research on Cryptography

Yuan-Ho Yao Apr. 2020-Mar. 2021

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

Yao-Ting Lin Jan. 2020-Present

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

Shiuan Fu Dec. 2019-Present

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

Yi-Hsin Ma Jul. 2019-Apr. 2021

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

Yu-Ching Shen Jun. 2019-Present

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

Yi Lee Mar. 2019-Nov. 2020

- M.S., Department of Mathematics, Johns Hopkins University.
- PhD student, University of Technology Sydney
- Research on Cryptography, Quantum Information

Chun-Hsiang Chan Sep. 2018-Jul. 2019

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

Hao-Ting Wei Sep. 2018-Mar. 2019

- M.S., Department of Industrial Engineering, National Tsing Hua University.
- Research on Algorithms

Hao Chung Aug. 2018-Feb. 2021

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

Kuan-Yi Ho Dec. 2017-Aug. 2018

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

Chun-Peng Chang Sep. 2017-Apr. 2018

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

Jyun-Jie Liao Nov. 2016-Aug. 2018

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

Yin-Hsun Huang Nov. 2016-Jul. 2017

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

Chi-Ning Chou Jun. 2016-Jul. 2017

- B.S., Computer Science, National Taiwan University
- Research on Computational Complexity and Algorithms

Yan-Lin Chen Jul. 2016-Jun. 2020

- M.S., Electrical Engineering, National Taiwan University
- PhD student, Centrum Wiskunde en Informatica
- Research on Quantum Information and Cryptography

Tsung-Hsuan Hung Jul. 2015-Jan. 2017

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

Wei-Kai Lin Nov. 2014-Jul. 2016

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

Graduate Students

Tong-Nong Lin Aug. 2018-Jul. 2019

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

Mi-Ying Huang Jul. 2018-Present

- M.S. Student, Department of Electrophysics, National Chiao Tung university
- Research on quantum cryptography, complexity theory, and quantum information

Hsien-Ming Pan Sep. 2018-June. 2020

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

I-Hung Hsu Sep. 2017-Jun. 2019

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

Tsung-Hsuan Hung Feb. 2017-Aug. 2018

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

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

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

Chiao-Hsun Wang Sep. 2015-Aug. 2017

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

Yan-Lin Chan (co-advised) May 2014-Jun. 2016

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

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

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

Undergraduate Students

Hsi Tai Jul. 2020-Dec. 2020

- B.S., Computer Science, University of Michigan
- Research on Cryptography

Tai-Ning Liao Sep. 2018-Jan. 2020

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

Chun-Chi Wu Sep. 2018-Feb. 2019

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

Tun-Yi Chang Feb. 2016-Jul. 2017

- B.S., Department of Physics, National Taiwan University

Kuan-Yi Ho Jul. 2016-Jul. 2017

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

Chi-Ning Chou (summer intern) Jul. 2015-Aug. 2015

- Computer Science, National Taiwan University
- Research on Cryptography

VISITORS HOSTED

Short Term Visitors

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 Brakersk (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 Komargodsk (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 Cohan (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

On the Power of Hybrid Classical and Low-depth Quantum Computation

Joint CQSE-NCTS-CASTS-CTP Seminar, NTU , Taiwan 04/16/2021

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

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), join 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