Kai-Min Chung

Cornell University, Computer Science Dept. (401) 578-1856
Upson Hall 4108, chung@cs.cornell.edu
Ithaca, NY 14850 http://www.cs.cornell.edu/~chung/

Research Interests

Cryptography and Complexity Theory

Current Position

Assistant Researcher Sept. 2013 – Present
Institute of Information Science, Academia Sinica, Taiwan

Previous Position

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
- GPA: 3.92/4.00; Ranked 3rd out of 81.

Honors and Awards

Simons Postdoctoral Fellowship 2010
Award for Postdocs in Mathematics, Theoretical Physics, and Theoretical Computer Science.

Certificate of Distinction in Teaching 2009
Award for outstanding teaching fellows

Fellow of the Phi Tau Phi Scholastic Honor Society 2003
In recognition of the exceptional performance of undergraduate students in Dept. of CSIE, NTU

Asia Champion of ACM International Collegiate Programming Contest 2001
With H.-R. Hsu and W.-C. Wu, Coach: C.S. Fuh.

Silver Medal of 10^{th} International Olympiad in Informatics 1998

SYNERGISTIC ACTIVITIES

Program Committee

- 33rd Annual International Cryptology Conference (CRYPTO 2013).
- 11th Theory of Cryptography Conference (TCC 2014).

Journal Refereeing

Journal of Cryptology, SIAM Journal on Computing, IEEE Transactions on Neural Networks

Conference Refereeing

CCC 2013 & 2012, TCC 2013 & 2012 & 2011, FOCS 2012, Asiacrypt 2012 & 2011, ICALP 2012, CRYPTO 2011 & 2009, RANDOM 2011, STOC 2007

TEACHING EXPERIENCE

Teaching Fellow, CS225 Pseudorandomness Spring 2009

Taught by Prof. Salil Vadhan

Received **Certificate of Distinction in Teaching**

I interacted with students closely through holding biweekly sections and office hours. I also took the responsibility of grading problem sets.

Teaching Fellow, CS225 Pseudorandomness Spring 2007

Taught by Prof. Salil Vadhan

PUBLICATIONS

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

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

[22] *Simultaneous Resettability from One-Way Functions*
Kai-Min Chung and Rafail Ostrovsky and Rafael Pass and Ivan Visconti
To appear in proceedings of the 54th Annual IEEE Symposium on Foundations of Computer Science (**FOCS**), 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 Award; 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.

• MANUSCRIPTS

[3] *On the (Im)Possibility of Tamper-Resilient Cryptography: Using Fourier Analysis in Computer Viruses*
Per Austrin and Kai-Min Chung and Mohammad Mahmoody and Rafael Pass and Karn Seth
Manuscript, 2013

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

[1] *From Weak To Strong Zero Knowledge Using a New Non-Black-Box Simulation Technique*
Kai-Min Chung and Edward Lui and Rafael Pass
Manuscript, 2012.

TALKS

Interactive Coding, Revisited
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