

Chiu-Yuen Koo
cykoo1@gmail.com
<http://www.cs.umd.edu/~cykoo/>

Research Interests

Cryptography, Distributed Computing and Algorithms.

Education

University of Maryland

Ph.D., Computer Science, Aug. 2007

Advisor: Professor Jonathan Katz

Title of Dissertation: Studies on Fault-Tolerant Broadcast and Secure Computation.

University of Hong Kong

Bachelor of Engineering in Computer Engineering, Dec. 2001 (First Class Honors)

Employment History

Google

Software Engineer in the security group (Oct. 2007 – Present)

Institute for Pure and Applied Mathematics (IPAM), UCLA

Fellow for the Fall 2006 Program on Securing Cyberspace:

Application and Foundations of Cryptography and Computer Security (Sept. 2006 – Dec. 2006)

Bell Labs, Lucent Technologies

Summer Intern (June 2006 – Aug. 2006)

Mentor: Dr. Juan Garay

University of Maryland

Graduate Research Assistant, Department of Computer Science (Aug. 2003 – June 2006, Jan. 2007 – Aug. 2007)

Supervisor: Professor Jonathan Katz

University of Maryland

Graduate Teaching Assistant, Department of Computer Science (Aug. 2001 – Jan. 2004)

University of Hong Kong

Summer Research Assistant, Department of Computer Science (Summer 2000, 2001)

Supervisor: Professor Tak-Wah Lam

Publications

Journal Articles

1. **On Expected Constant-Round Protocols for Byzantine Agreement.** With Jonathan Katz. *In submission.*
2. **On Constructing Universal One-Way Hash Functions from Arbitrary One-Way Functions.** With Jonathan Katz. *In submission.*
3. **Reducing Complexity Assumptions for Statistically-Hiding Commitment.** With Iftach Haitner, Omer Horvitz, Jonathan Katz, Ruggero Morselli and Ronen Shaltiel. Accepted to *Journal of Cryptology* (pending revisions).
4. **Extra Processors versus Future Information in Optimal Deadline Scheduling.** With Tak-Wah Lam, Tsuen-Wan “Johnny” Ngan and Kar-Keung To. *Theory of Computing Systems*, 37(3), pages 323-341, May 2004 (special issue for SPAA 2002).
5. **Competitive Deadline Scheduling via Additional or Faster Processors.** With Tak-Wah Lam, Tsuen-Wan “Johnny” Ngan and Kar-Keung To. *Journal of Scheduling* (special issue on on-line scheduling), 6(2), pages 213-223, March 2003.
6. **On-line Scheduling with Tight Deadlines.** With Tak-Wah Lam, Tsuen-Wan “Johnny” Ngan, Kunihiko Sadakane and Kar-Keung To. *Theoretical Computer Science (TCS)*, 295(1-3), pages 251-261, February 2003 (special issue for MFCS 2001).

Articles in Refereed Conferences

1. **Improving the Round Complexity of ‘Round-Optimal’ VSS.** with Jonathan Katz and Ranjit Kumaresan. *In submission.*
2. **Round Complexity of Authenticated Broadcast with a Dishonest Majority.** With Juan Garay, Jonathan Katz and Rafail Ostrovsky. *IEEE Symposium on Foundations of Computer Science (FOCS) 2007*, to appear.
3. **Round-Efficient Secure Computation in Point-to-Point Networks.** With Jonathan Katz. In *Advances in Cryptology - EUROCRYPT 2007*, pages 311-328
4. **Concurrently-Secure Blind Signatures without Random Oracles or Setup Assumptions.** With Carmit Hazay, Jonathan Katz and Yehuda Lindell. In the *4th Theory of Cryptography Conference (TCC 2007)*, pages 323-341.
5. **On Expected Constant-Round Protocols for Byzantine Agreement.** With Jonathan Katz. In *Advances in Cryptology - CRYPTO 2006*, pages 445-462.
6. **Reliable Broadcast in Radio Networks: The Bounded Collision Case.** With Vartika Bhandari, Jonathan Katz and Nitin Vaidya. In Proceedings of the *25th ACM SIGACT-SIGOPS Symposium on Principles of Distributed Computing (PODC)*, pages 258-264, 2006.
7. **Secure Computation with Partial Message Loss.** In the *3rd Theory of Cryptography Conference (TCC 2006)*, pages 502-521.

8. **Reducing Complexity Assumptions for Statistically-Hiding Commitment.** With Iftach Haitner, Omer Horvitz, Jonathan Katz, Ruggero Morselli and Ronen Shaltiel. In *Advances in Cryptology - EUROCRYPT 2005*, pages 58-77.
9. **Broadcast in Radio Networks Tolerating Byzantine Adversarial Behavior.** In Proceedings of the *23rd ACM SIGACT-SIGOPS Symposium on Principles of Distributed Computing (PODC)*, pages 275-282, 2004.
10. **Extra Processors versus Future Information in Optimal Deadline Scheduling.** With Tak-Wah Lam, Tsuen-Wan “Johnny” Ngan and Kar-Keung To. In Proceedings of the *14th ACM Symposium on Parallel Algorithms and Architectures (SPAA)*, pages 133-142, 2002.
11. **On-line Scheduling with Tight Deadlines.** With Tak-Wah Lam, Tsuen-Wan “Johnny” Ngan and Kar-Keung To. In Proceedings of the *26th International Symposium on Mathematical Foundations of Computer Science (MFCS)*, pages 464-473, 2001.

Honors and Awards

- University of Maryland, Dean’s Fellowship Award for excellence in Research, 2005
- Dean’s Honour List, Faculty of Engineering, University of Hong Kong (1998-2001)
- Recipient of the Zodiac/Seagate Scholarships (1998-1999, 2000-2001)
- ACM International Collegiate Programming Contest (ICPC)
 - 29th place (out of 64 teams) in the 2001 ACM World Finals, Vancouver, Canada
 - 3rd place in the 2000 ACM Asia Programming Contest, Hong Kong
- ACM-HK Scholastic Programming Contest
 - Champion in 2000, 2nd Runner-up in 2001
- Bronze medal in the 10th International Olympiad in Informatics (IOI), Setubal, Portugal, 1998

Invited Talks

- Workshop On Foundations of Secure Multi-Party Computation and Zero-Knowledge and its Applications (UCLA/IPAM): “Round-Efficient Multi-Party Computation in Point-to-Point Networks”, November 2006.
- Bell Labs, Lucent Technologies: “On Expected Constant-Round Protocols for Byzantine Agreement”, August 2006.
- IBM T.J. Watson Research Center: “On Expected Constant-Round Protocols for Byzantine Agreement”, July 2006.

Conference Talks

- Eurocrypt '07: “Round-Efficient Secure Computation in Point-to-Point Networks”, May 2007.
- Crypto '06: “On Expected Constant-Round Protocols for Byzantine Agreement”, August 2006.
- TCC '06: “Secure Computation with Partial Message Loss”, March 2006.
- PODC '04: “Broadcast in Radio Networks Tolerating Byzantine Adversarial Behavior”, July 2004.
- SPAA '02: “Extra Processors versus Future Information in Optimal Deadline Scheduling”, August 2002.

Teaching Experience

- Teaching Assistant, University of Maryland, Aug. 2001 – Jan. 2004
- Trainer, Hong Kong Olympiad in Informatics (HKOI) training team, 1998 – 2001

Professional Activities

- Journal Reviews. ACM Transactions on Algorithms (TALG), Journal of Computer and System Sciences (JCSS), International Journal of Foundations of Computer Science (IJFCS), International Journal of Wireless and Mobile Computing (IJWMC), Distributed Computing
- Conference Reviews. Asiacrypt 2004, Crypto 2005, 2006, Eurocrypt 2006, ACM Symposium on Principles of Distributed Computing (PODC) 2005, 2006, Theory of Cryptography Conference (TCC) 2006, 2007, 2008 The International Conference on Dependable Systems and Networks (DSN) 2006, SKLOIS Conference on Information Security and Cryptology (Inscrypt) 2006, ACM Symposium on Theory of Computing (STOC) 2007, International Colloquium on Automata, Languages and Programming (ICALP) 2007.

References

Professor Jonathan Katz

Department of Computer Science and UMIACS
University of Maryland
College Park, MD 20742, USA
jkatz@cs.umd.edu

Dr. Juan Garay

Security Technology Research Department
Bell Labs – Lucent Technologies
600 Mountain Ave, Murray Hill, NJ 07974, USA
garay@research.bell-labs.com

Professor Rafail Ostrovsky

Department of Computer Science
University of California
Los Angeles, CA 90095, USA
rafail@cs.ucla.edu

Professor Tak-Wah Lam

Department of Computer Science
University of Hong Kong
Hong Kong
twlam@cs.hku.hk

Citizenship and Immigration Status

Citizen of Hong Kong SAR.
US Immigration Status: Student Visa (F-1).