Ke Yang

Computer Science Department
Carnegie Mellon University
5000 Forbes Ave.
Pittsburgh, PA 15213
(412) 268-3069

331 Devonshire St. Apt A2
Pittsburgh, PA 15213
(412) 688-0807
yangke@cs.cmu.edu

Objective To find a permanent position in research labs or research-oriented universities, or a post-doctorate position.

Research Interests My research interests mainly lie in theoretical computer science, including cryptography and computer security, quantum information theory and quantum computation, machine learning, and computational complexity.

Education

- **Carnegie Mellon University** Pittsburgh, PA, USA
  Ph.D. candidate in Computer Science.
  Thesis adviser: Steven Rudich.
- **Carnegie Mellon University** Pittsburgh, PA, USA
  M.S. in Computer Science, May 2002.
- **Tsinghua University** Beijing, China
  B. Eng. in Computer Science and Technology, June 1998.

Awards and Honors

- *E.M.Gold Award* for best paper by student authors, the *12th International Conference on Algorithmic Learning Theory*, 2001.
- Carnegie Mellon University School of Computer Science Alumni Fellowship, 2001.
- Carnegie Mellon University Doctorate Fellowship, 1998 – 2003.
- Graduated with Honor from Tsinghua University, 1998.
- *Ling Jia-Qiao Scholarship* for excellence for Mathematics study, 1997.
- *Tsinghua-German Scholarship* for excellence in German study, 1996.
- *Tsinghua-JinLing Scholarship* for outstanding undergraduate research, 1996.
- *Tsinghua-Samsung Scholarship* for outstanding student (top 5 in class of 180), 1996.
- Honor of outstanding student for excellence in performance, 1995.
- *Tsinghua-IBM Scholarship* for outstanding student (top 5 in class of 180), 1995.
- *Shi-NianDe Scholarship* for outstanding student (top 5 in class of 180), 1994.
- *Gold Medal (First Prize)* in the 34th International Mathematical Olympiads (IMO), ranking No. 8 among about 406 contestants world-wide, 1993.
- First Prize in the Chinese Mathematical Olympiads (the highest-level mathematics competition in China), 1993.

List of Papers (reverse chronological)

1. T. Liu, *K. Yang*, A. W. Moore.
   The IOC algorithm: Efficient Many-Class Non-parametric Classification for High-Dimensional Data.
   Submitted.

2. J. Garay, P. MacKenzie, *K. Yang*.
   Efficient and Secure Multi-Party Computation with Faulty Majority and Complete Fairness.
   Submitted.

3. A. Ambainis, *K. Yang*.
   Towards the Classical Communication Complexity of Entanglement Distillation Protocols with Incomplete Information.
   To appear in the *19th Aunnual IEEE Conference of Computational Complexity (CCC 2004)*, Amherst, MA.

4. L. Kissner, A. Oprea, M. Reiter, D. Song, *K. Yang*.
   Private Push and Pull with Applications to Anonymous Communication.
   Submitted.

5. P. MacKenzie, *K. Yang*.
   On Simulation-Sound Trapdoor Commitments.
   To appear in *Eurocrypt 2004*, Interlaken, Switzerland, 2004.

6. *K. Yang*.
   On the (Im)possibility of Non-interactive Correlation Distillation.
   To appear in *Latin American Theoretical INformatics (LATIN 2004)*, Buenos Aires, Argentina, 2004.

7. J. Garay, P. MacKenzie, *K. Yang*.
   Efficient and Universally Composable Committed Oblivious Transfer and Applications.
   Appeared in *Theory of Cryptography Conference (TCC '04)*, Cambridge, MA, pp. 297-316, 2004.

8. P. MacKenzie, M. Reiter, *K. Yang*.
   Alternatives to Non-Malleability: Definitions, Constructions and Applications.
   Appeared in *Theory of Cryptography Conference (TCC '04)*, Cambridge, MA, pp. 171-190, 2004.

9. A. Blum, *K. Yang*.
   On Statistical Query Sampling and NMR Quantum Computing.
   Appeared in the *18th Annual IEEE Conference of Computational Complexity (CCC 2003)*, Århus, Denmark, pp. 194-205, 2003.

10. J. Garay, P. MacKenzie, *K. Yang*.
    Strengthening Zero-Knowledge Protocols using Signatures.
    In *Eurocrypt 2003*, Warsaw, Poland, LNCS 2656, pp.177-194, 2003.

11. *K. Yang*.
    New Lower Bounds for Statistical Query Learning.
    Appeared in the *Fifteenth Annual Conference on Computational Learning Theory (COLT 2002)*, Sydney, NSW, Australia, LNAI 2375, pp. 229-243, 2002.

12. M. Blum, R. Rue, *K. Yang*.
    On the Complexity of MAX/MIN/AVRG Circuits.
    CMU SCS Technical Report, CMU-CS-02-110, 2002.

13. A. Ambainis , A. Smith, *K. Yang*.
    Extracting Quantum Entanglement (General Entanglement Purification Protocols).
    Appeared in the *IEEE Conference of Computational Complexity (CCC 2002)*, Montréal, Quebéc, Canada, pp. 103-112, 2002.

14. *K. Yang*.
On Learning Correlated Boolean Functions Using Statistical Query.
Appeared in the *Twelfth International Conference on Algorithmic Learning Theory (ALT 2001)*, Washington, DC, LNAI 2225, pp. 59-76, 2001.

15. B. Barak, O. Goldreich, R. Impagliazzo, S. Rudich, A. Sahai, S. Vadhan, *K. Yang*.
On the (Im)possibility of Obfuscating Programs.
In the *21st Annual International Cryptology Conference (CRYPTO 2001)*, pp. 1 – 18, 2001.

16. L. Huang, X. Wang, F. Xie, *K. Yang*.
Formal Authentication Based on Intruder's Role Impersonate (in Chinese).
Appeared *Journal of Tsinghua University*, July, 2001.

17. *K. Yang*.
Integer Circuit Evaluation is PSPACE-complete.
Appeared in the *IEEE Conference of Computational Complexity (CCC 2000)*, Florence, Italy, pp. 204 - 213, 2000. Journal version at *Journal of Computer and System Sciences*, 63, 288–303 (2001).

18. *K. Yang*, X. Lin, Y. Dai
Minimal Size of $(2, n)$ Data Sharing Scheme Under XOR Operation (in Chinese).
Appeared in *Journal of Tsinghua University*, May, 1998.

Selected Presentations

1. "**On Statistical Query Sampling and NMR Quantum Computing**."
Bell Labs, Lucent Technologies, Murray Hill, NJ, 2003.

2. "**On Statistical Query Sampling and NMR Quantum Computing**."
The *18th Annual IEEE Conference of Computational Complexity (CCC 2003)*, Århus, Denmark, 2003.

3. "**Strengthening Zero-Knowledge Protocols using Signatures**."
New York Univerity, New York, 2003.

4. "**Strengthening Zero-Knowledge Protocols using Signatures**."
Eurocrypt 2003, Warsaw, Poland, 2003.

5. "**New Lower Bounds for Statistical Query Learning**."
The *Fifteenth Annual Conference on Computational Learning Theory*, Sydney, New South Wales, Australia, 2002.

6. "**On the (Im)possibilities of Obfuscating Programs**."
IBM T.J. Watson Research Center, Yorktown Heights, NY, 2002.

7. "**On the (Im)possibilities of Obfuscating Programs**."
Bell Labs, Lucent Technologies, Murray Hill, NJ, 2002.

8. "**Extracting Quantum Entanglement (General Entanglement Purification Protocols)**."
The *17th Annual IEEE Conference of Computational Complexity (CCC2002)*, Montréal, Quebéc, Canada, 2002

9. "**Issues for Chinese CAPTCHAs**."
Xerox Palo Alto Research Center (PARC), Palo Alto, CA, 2002.

10. "**On the (Im)possibilities of Obfuscating Programs**."
Carnegie Mellon University, Pittsburgh, PA, 2001.

11. "**Code Obfuscation: A Definition game**."
University of Toronto, Toronto, Ontario, Canada, 2000.

12. "**Code Obfuscation: A Definition game**."
Microsoft Research, Richmond, WA, 2000.

13. "**Integer Circuit Evaluation is PSPACE-complete**."
The *15th Annual IEEE conference of computational complexity (CCC2000)*, Florence, Italy, 2000.

Refereed Journal Publications

1. *K. Yang*.
New Lower Bounds for Statistical Query Learning.
Invited to the *Journal of Computer and System Science* (manuscript in preparation).

2. *K. Yang*.
On Learning Correlated Functions Using Statistical Query.
Invited to the *Theoretical Computer Science* (manuscript in preparation).

3. *K. Yang*.
Integer Circuit Evaluation is PSPACE-complete.
Appeared in the *Journal of Computer and System Science*, vol. 63, 288-303 (2001).

Working Experiences

- **Summer Intern/Technical Consultant** June 2002 – Sept. 2002, June. 2003 – Present
Bell Labs / Lucent Technologies Murray Hill, NJ

  My work in Bell Labs in this term consists both theoretical cryptography and computer security.

  Fair Multi-Party Computation with Faulty Majority We constructed the first completely fair and efficient multi-party computation protocol with provable security in the face of faulty majority. We also gave a particularly efficient protocol for the *generalized* socialist millionaires' problem.

  Alternatives to Non-Malleability We investigated the notion of non-malleability with an eye towards whether this is necessary. We presented two alternative formations of this concept and proved that these alternatives provide the same level of security as the old definitions, and admit more efficient constructions.

  Extended Commited Oblivious Transfer We proposed a new cryptographic primitive known as *extended commmitted oblivious transfer (ECOT)*, that is, informally, a combination of the bit commitment, the oblivious transfer, and the zero-knowledge proof. We constructed an efficient protocol that securely realizes ECOT. We also showed how to construct efficient and universally composable two-party and multi-party computation protocols using ECOT as a building block.

  Simulation-Sound Trapdoor Commitments We proposed a new primitive, known as *simulation-sound trapdoor commitments*. This primitive has found many applications in constructing secure protocols very efficiently. We also investigated its relation to non-malleable commitments.

  Strengthening Zero-Knowledge Protocols Using Signatures We constructed efficient, concurrently secure, non-malleable, and universally composable zero-knowledge protocols. Our protocols are efficient and practical. We used a novel technique using digital signatures in our construction.

  Obfuscation/Temper Resistance Library I wrote a library that provides temper resistance functionality to programs. The library can be easily plugged into existing codes to enforce the integrity of the codes and data. The library is (reasonably) obfuscated so that it is hard to remove.

  References: Juan Garay, Philip MacKenzie, Eric Grosse.

- **Summer Intern** June. 2000 – Sept. 2000
Akamai Technologies Cambridge, MA

  I worked in two independent projects during my three months internship.

  Prototype High-Performance Distributed Web Server I developed a prototype distributed web-server. It consists of multiple standard Linux PCs connected by a Giga-bit switch, which has a much lower latency than the typical 100Mb Ethernet cards. As a result, the web-server has a very good performance.

Tera-Byte Data Mining We developed a multi-threaded data-mining infrastructure for massive data analysis and large-scale simulation. It exploits the multi-threaded programming on an SMP machine, and is capable of processing terabytes of data and billions of objects. Akamai accumulates tens of gigabytes of data (compressed) daily and our infrastructure is able to process them in almost real-time. We used the infrastructure to perform automated data flow analysis on Akamai's FreeFlow service and reporting. We also performed various simulations on network caching using this infrastructure.

References: Bradley Kuszmaul, Bruce Maggs, Harald Prokop, Ramesh Sitaraman.

- **Part-time Software Engineer** Mar. 1997 – Jun. 1997
  Teng Tu China Corp Beijing, China

  We developed MapEditor, an interactive platform for developing RPGs (Role Playing Games). It is Windows-based, user-friendly, and easy to use. Our product, MapEditor, was used by the artists within Teng Tu to develop the game "The Monkey King" and boosted the efficiency greatly.

  References: Ma Quan, Tao Chao-Quan.

Teaching Experiences

- **Teaching Assistant** Sept. 2001 – Dec. 2001
  Computer Science Department, Carnegie Mellon University Pittsburgh, PA

  I was the teaching assistant to 15-855, "An Intensive Introduction to Computational Complexity," a graduate level course on computational complexity theory.

  Reference: Steven Rudich.

- **Teaching Staff** July 2001 – Aug. 2001
  Andrew's Leap, Carnegie Mellon University Pittsburgh, PA

  I worked with a small group of talented junior high school and high school students to conduct original mathematical research.

  Reference: Steven Rudich.

- **Teaching Assistant** Feb. 2000 – May. 2001
  Computer Science Department, Carnegie Mellon University Pittsburgh, PA

  I was the teaching assistant to 15-251, "Great Theoretical Ideas in Computer Science," an undergraduate level course on theoretical computer science.

  References: Steven Rudich, Bruce Maggs.

- **Teaching Assistant** Sep. 1999 – Dec. 1999
  Computer Science Department, Carnegie Mellon University Pittsburgh, PA

  I was the teaching assistant to 15-452, "Formal Language, Automata, and Computability," an undergraduate level course on advanced theoretical computer science.

  References: Lenore Blum, Manuel Blum.

- **Teaching Staff** July 1999 – Aug. 1999
  Andrew's Leap, Carnegie Mellon University Pittsburgh, PA

  I lectured on programming in C++ to about 20 talented high school students. The students gained solid knowledge on the C++ programming and were able to finished a quite sophisticated project by the end of the program.

  Reference: Steven Rudich.

Biographical Information I am a Chinese citizen (People's Republic of China), currently holding F-1 visa in the US. I was born on May 5th, 1976 in Gansu, China. I speak native Chinese (Mandarin) and fluent English.

References

- **Prof. Steven Rudich**
  Computer Science Department, Carnegie Mellon University.
  5000 Forbes Ave. Pittsburgh, PA 15213, USA. (412) 268-7885
  rudich@cs.cmu.edu

- **Prof. Manuel Blum**
  Computer Science Department, Carnegie Mellon University.
  5000 Forbes Ave. Pittsburgh, PA 15213, USA. (412) 268-3742
  mblum@cs.cmu.edu

- **Prof. Avrim Blum**
  Computer Science Department, Carnegie Mellon University.
  5000 Forbes Ave. Pittsburgh, PA 15213, USA. (412) 268-6452
  avrim@cs.cmu.edu

- **Dr. Philip MacKenzie**
  Bell Labs, Lucent Technologies.
  600 Mountain Avenue, 2B-429 Murray Hill, NJ 07974, USA. (908) 582-7625
  philmac@lucent.com