Yitao Duan

600 Gooding Way # 616 Bldg 143
Albany, Ca 94706
(510)525-7537 (H), (510)517-7838 (C)
duan@cs.berkeley.edu
http://www.cs.berkeley.edu/~duan

Computer Science Division
EECS Department
387 Soda Hall
University of California
Berkeley, CA 94720-1776

EDUCATION

Ph.D.	**University of California, Berkeley** Computer Science, May 2007, GPA: 3.96/4.0, Major GPA: 4.0/4.0
M.S.	**Beijing University of Aeronautics and Astronautics (BUAA)** Aircraft Design, May 1997, GPA: 3.86/4.0
B.S.	**Beijing University of Aeronautics and Astronautics (BUAA)** Aircraft Design, July 1994, GPA: 3.89/4.0

DISSERTATION

P4P: A Practical Framework for Privacy-Preserving Distributed Computation
(Advisor: Professor John Canny)

RESEARCH INTERESTS

Practical privacy and security technologies for a variety of applications, such as ubiquitous computing, collaborative and distributed computation, data mining, etc., applied cryptography, operating systems.

PROFESSIONAL EXPERIENCE

Research Assistant, Berkeley Institute of Design (BID), Department of Electrical Engineering and Computer Science, University of California, Berkeley (2002 – present)

Primary researcher of the Peers for Privacy (P4P) project. Developed algorithms and protocols for efficient privacy-preserving distributed computation. Implemented the P4P code (in Java) including the vector aggregation protocol and a number of cryptographic primitives, such as bit commitment proof, zero-knowledge proof that the L2-norm of a vector is bounded by a given limit, etc. More information available at http://www.cs.berkeley.edu/~duan/research/p4p.html.

Intern, IBM Almaden Research Center, California (summer and fall 2002)

Worked on Distributed Storage Tank (DST) project, a wide-area distributed storage system. Designed and built a prototype system that integrates multiple DST systems located on different sites providing users with a uniform file system namespace.

Research Assistant, Berkeley Institute of Design (BID), Department of Electrical Engineering and Computer Science, University of California, Berkeley (09/1999 – 2002)

Worked on Smart Room Project, an intelligent, sensor-equipped space supporting efficient collaborative design activities. Responsible for deploying all key equipments including various sensors, an RFID reader, and a number of servers. Tasks cover hardware installation/configuration, software/protocol development, and system architecture design. The system involves programming on various platforms (Windows2000/98, Linux) and in various languages (C/C++, Java).

Research Assistant, Department of Mechanical Engineering, University of California, Berkeley (03/1998 – 12/1999)

Worked on UCB Improved Multinode Model of Human Physiology and Thermal Comfort. Participated in algorithm design. Implemented the Human Thermal Comfort Simulator in an object-oriented (OO) approach.

Software Engineer, Beijing Skyship Advanced Technology Co., Ltd. (01/1995 – 12/1997)

Designed and implemented control software (C/C++) for GPS Vehicle Security System, which was deployed in Xuchang, Henan Province, China. The system used GPS to track and monitor automobiles, providing various services for drivers.

Research Assistant, Beijing Univ. of Aeronautics and Astronautics (1994 – 1996)

Participated in algorithm research. Designed and implemented (using C++) Aircraft RCS Analysis System, which won Chinese Aviation Industry Prize in 1995.

PUBLICATIONS

- Yitao Duan, John Canny and Justin Zhan. **Efficient Privacy-Preserving Association Rule Mining: P4P Style**. To appear in IEEE Symposium on Computational Intelligence and Data Mining (CIDM 2007), April 1-5, 2007, Honolulu, Hawaii.
- Yitao Duan and John Canny. **Scalable Secure Bidirectional Group Communication**. To appear in INFOCOM 2007, May 6-12, 2007, Anchorage, Alaska, USA.
- Yitao Duan and John Canny. **From Commodity to Value: A Privacy-Preserving e-Business Architecture**. In 2006 IEEE International Conference on e-Business Engineering (ICEBE 2006), Oct. 24 - 26, Shanghai, China.
- Yitao Duan and John Canny. **Zero-knowledge Test of Vector Equivalence and Granulation of User Data with Privacy**. In 2006 IEEE International Conference on Granular Computing (GrC 2006), May 10 - 12, Atlanta, USA.

- Yitao Duan and John Canny. **How to Construct Multicast Cryptosystems Provably Secure against Adaptive Chosen Ciphertext Attack**. In RSA Conference 2006, Cryptographers' Track. February 13 - 17, 2006, McEnery Convention Center, San Jose, USA.
- Yitao Duan, Jingtao Wang, Matthew Kam, John Canny. **Privacy Preserving Link Analysis on Dynamic Weighted Graph**, Computational & Mathematical Organization Theory, Volume 11, Issue 2, Jul 2005, Pages 141 – 159.
- Yitao Duan, Jingtao Wang, Matthew Kam and John Canny. **A Secure Online Algorithm for Link Analysis on Weighted Graph**, SIAM Workshop on Link Analysis, Counterterrorism and Security, (at the SIAM Int. Conf. on Data Mining), Sutton Place Hotel, Newport Beach, California, USA, 23rd April, 2005.
- Yitao Duan and John Canny. **Protecting User Data in Ubiquitous Computing: Towards Trustworthy Environments**. Privacy-Enhancing Technologies (PET) 2004, Toronto, CA, May 2004.
- Ben Y. Zhao, Yitao Duan, Ling Huang, Anthony D. Joseph, and John D. Kubiatowicz, **Brocade: Landmark Routing on Overlay Networks**, IPTPS'02.
- Huizenga, C., Z. Hui, Y. Duan, E. Arens, **An Improved Multinode Model of Human Physiology and Thermal Comfort**. Proceedings of Building Simulation '99, Volume 1: 353-359.

TEACHING EXPERIENCE

- **Teaching Assistant**, UC Berkeley, CS 162 Operating Systems, Fall 2004
- **Teaching Assistant**, BUAA, several computer language and undergraduate algorithm courses, 1994 – 1997
- **Mentor**, SUPERB-IT (Summer Undergraduate Program in Engineering Research at Berkeley Information Technology), UC Berkeley, summer 2005
- **Mentor,** for undergraduate researchers, UC Berkeley, 2001 – 2004.

AWARDS AND HONORS

- ***CATIC*** Scholarship, 1992 –1994, First & second prizes, BUAA
- People's Scholarship, 1992 –1994, First & second prizes, BUAA
- ***Lizheng*** Scholarship (Awarded to outstanding first year students only), 1991, BUAA
- ***Excellent Student*** title, 1991 –1994 (top 5% of all the undergraduates in BUAA)
- ***Excellent Graduate*** title, 1995 (top 1% of 1995 graduates from Beijing universities)
- Championship in English contest, 1993, BUAA
- Second in computer programming contest, 1992, BUAA
- ***China Aviation Industry Prize*** (a nation-wide prize), 1995, Third Prize

SKILLS

- Language: English, Chinese
- Programming: C/C++, Java, FORTRAN, MIPs and x86 assembly, VHDL, MATLAB

REFERENCES

John Canny (Advisor)
Paul and Stacy Jacobs Distinguished Professor of Engineering
Department of Electrical Engineering and Computer Sciences
University of California, Berkeley

Email: jfc@cs.berkeley.edu
Tel: (510) 642-9955
Fax: (510) 643-1534

Postal Mail:
529 Soda Hall,
University of California, Berkeley
Berkeley, CA 94720-1776

Doug Tygar
Professor of Computer Science, UC Berkeley
Professor of Information Management, UC Berkeley
Adjunct Professor of Computer Science, CMU

Email: tygar@eecs.berkeley.edu, doug.tygar@gmail.com
Tel: (510) 643-7855
Fax: (815) 301-5497

Postal Mail:
Prof. Doug Tygar
UCB-SIMS 102 South Hall #4600
Berkeley, CA 94720-4600, USA

Justin Zhan
Heinz School Faculty
The Heinz School
Carnegie Mellon University

Email: justinzh@andrew.cmu.edu
Tel: 81-78-3606325
Fax: 81-78-360-1618

Postal Mail:
The Heinz School
Carnegie Mellon University
5000 Forbes Avenue WH 405
Pittsburgh, PA 15213-3890, USA