

# Dinghao Wu

## 1. Contact Information

Address: College of Information Sciences and Technology  
The Pennsylvania State University  
313E IST Building, University Park, PA 16802  
Phone: (814) 867-3612; Fax: (814) 865-6426  
E-mail: dinghao@psu.edu  
<http://www.cs.princeton.edu/~dinghao/>

## 2. Research Interests

Programming languages and compilers, computer security, concurrent programming and verification, program analysis and verification, model checking, and formal methods.

## 3. Education

Princeton University, Ph.D., Computer Science, 2005.  
Thesis: *Interfacing Compilers, Proof Checkers, and Proofs for Foundational Proof-Carrying Code*. (Advisor: Andrew W. Appel)  
Princeton University, M.A., Computer Science, 2002.  
Nanjing University, M.E., Computer Science, 1999.  
Thesis: *A State-Space Based Approach to the Specification and Verification of Hybrid Systems and Its Axiomatic Basis*. (Advisor: Jian Lü)  
Nanjing Institute of Chemical Technology, B.E., Chemical Engineering, with Honors, 1996.  
Thesis: *Numerical Simulation of Free Turbulent Jets*. (Advisor: Daiqing Zhao)

## 4. Professional Appointments and Service

College of Information Sciences and Technology, The Pennsylvania State University, 2009–present.  
Microsoft Center for Software Excellence, Redmond, WA. Research engineer, 2005–2009.  
Princeton University, Princeton, NJ. Research and teaching assistant, 2000–2005.  
Microsoft Research, Redmond, WA. Summer research intern, Summer 2003 & 2004.  
Nanjing University, Nanjing, China. Research and teaching assistant, 1996–1999.  
Class President, Nanjing Institute of Chemical Technology, 1993–1996.  
Editor in Chief, Blackboard Bulletin of Nanjing Institute of Chemical Technology, 1992–1993.

## 5. Awards and Honors

Distinguished Graduate Student Award, Nanjing University, 1998.  
Distinguished Student Award, Nanjing Institute of Chemical Technology, 1995.  
Award for Excellence in Organizing Student Activities, Nanjing Institute of Chem. Tech., 1993, 94, 95.  
Honorable Mention, National Mathematical Contest in Modeling (MCM), Chinese Society for Industrial and Applied Mathematics, 1994. (with Miao Li and Ji Zhou, team advisor: Guoqing Liu)  
University Scholarship, Nanjing Institute of Chemical Technology, 1992–1996.  
Numerous awards on Chinese calligraphy, 1989–1992.

## 6. Research Experience

- **Static analysis and verification of web service code**  
Center for Software Excellence, Microsoft, March 2008–2009.  
We have built infrastructure and tools that apply static analysis on web services such as JavaScript code to address problems such as web site performance, localizability, service reliability, and security vulnerabilities. Our tools have caught bugs on localization and security such as Cross-Site Scripting (XSS) attacks in production code.
- **Static analysis of concurrency on the Windows source Code**  
Center for Software Excellence, Microsoft, March 2007–March 2008. (with Jason Yang)

Apply static analysis on the Windows source code to find concurrency errors such as race conditions and deadlocks. The tool, called EspC, has been deployed and applied to a very large-scale software development—Windows 7, and has found and fixed hundreds of bugs. A paper describing the static analysis and automated source code annotation inference techniques can be found in the publication section.

- **Testing and verification research on the Windows binary code**

Center for Software Excellence, Microsoft, August 2005–March 2007.

- Project 1: Automated test case generation via static program analysis on the Windows binary code to improve code coverage;
- Project 2: Automatic program annotation inference on binary code;
- Project 3: Exception handling error detection via static analysis on binary code. This project has found subtle bugs in production code.

- **Foundational Proof-Carrying Code (FPCC)**

Princeton University, June 2000–June 2005. (with Andrew Appel, et al.)

- Designed a low-level typed assembly language LTAL;
- Built a machine-checkable soundness proof of LTAL;
- Built a foundational proof checker Flit;
- Maintained the FPCC/ML compiler (type-preserving, proof-generating) since 2003;
- Published 3 papers in PLDI, PPDP, and VMCAI.

- **Heap abstraction and refinement using separation and dynamic program slicing**

Microsoft Research, Summer 2004. (with Shaz Qadeer)

- Proposed a novel heap abstraction scheme called  $\omega$ -abstraction;
- Implemented the  $\omega$ -abstraction and refinement in the software model checker Zing;

- **KISS: Debugging concurrent programs with sequential analysis**

Microsoft Research, Summer 2003. (with Shaz Qadeer)

- Proposed a novel technique to verify concurrent programs with sequential analysis;
- Implemented a precise static race detector based on the software model checker SLAM using the KISS technique;
- Found some serious race conditions in the Windows device drivers;
- Published a paper in PLDI 2004;
- Filed a patent application, titled “Data Race Detection Using Sequential Program Analysis”;
- The KISS project was started summer 2003 with Shaz Qadeer, and reviewed summer 2004 by Bill Gates;
- The KISS technique has been implemented in the Static Driver Verifier (SDV, the product version of SLAM), which is being released as part of Windows Vista and is now routinely used to check Windows Device Drivers.

- **Specification and verification of hybrid systems**

Nanjing University, 1998–1999. (with Jian Lü)

- Proposed a state space based decomposition approach;
- Designed a logic basis for this approach based on Hoare logic;
- Mechanically verified the soundness of the extended Hoare logic in PVS;
- Published 2 papers.

- **DD-VDM++**, Nanjing University, 1996–1999.

(with Jian Lü, Dajun Yang, and Ming Zhang)

- Designed a wide spectrum language/tool supporting systematic and rigorous software development (based on VDM and VDM++).

- **Radar data processing system**

Nanjing Institute of Chemical Technology, 1993. (with Guoqing Liu and Ji Zhou)

- Designed a new wave filter algorithm;
- Implemented a radar data processing system;
- The system was used in some meteorological observation stations in Jiangsu Province, China;
- Published a conference paper.
- **Numerical simulation of free turbulent jets**  
Nanjing Institute of Chemical Technology, 1996. (with Daiqing Zhao)

## 7. Teaching Experience

- Assistant in Instruction, Department of Computer Science, Princeton University.
  - COS111 Computers and Computing (Spring 2002)
  - COS109 Computers in Our World (Fall 2001)
- Advisor for Summer Programming Experience (SPE) program, Princeton University.
  - Advising a freshman programming project (Summer 2001)
- Volunteer Teacher, Princeton Chinese Language School.
  - Teaching children the game of Go (Wei-Qi) (Fall 2002)
- Teaching Assistant, Department of Computer Science, Nanjing University.
  - UNIX and C (Spring 1997)

## 8. Publications

- [1] “Detecting Data Race and Atomicity Violation via Typestate-Guided Static Analysis,” (Yue Yang, Anna Gringauze, Dinghao Wu, and Henning Rohde), Technical Report MSR-TR-2008-108, Microsoft Research, August 2008.
- [2] “KISS: Keep It Simple and Sequential,” (Shaz Qadeer and Dinghao Wu), *Proceedings of the 2004 ACM SIGPLAN Conference on Programming Language Design and Implementation (PLDI 2004)*, Washington DC, June 9–11, 2004, 14–24.
- [3] “Construction of a Semantic Model for a Typed Assembly Language,” (Gang Tan, Andrew W. Appel, Kedar N. Swadi, and Dinghao Wu), *Proceedings of the Fifth International Conference on Verification, Model Checking, and Abstract Interpretation (VMCAI 2004)*, Springer-Verlag Lecture Notes in Computer Science (LNCS 2937), Venice, Italy, January 2004, 30–43.
- [4] “Foundational Proof Checkers with Small Witnesses,” (Dinghao Wu, Andrew W. Appel, and Aaron Stump), *Proceedings of the Fifth ACM-SIGPLAN International Conference on Principles and Practice of Declarative Programming (PPDP 2003)*, Uppsala, Sweden, August 27–29, 2003, 264–274.
- [5] “A Provably Sound TAL for Back-end Optimization,” (Juan Chen, Dinghao Wu, Andrew W. Appel, and Hai Fang), *Proceedings of the 2003 ACM SIGPLAN Conference on Programming Language Design and Implementation (PLDI 2003)*, San Diego, California, June 8–11, 2003, 208–219.
- [6] (in Chinese) “On Theoretical Basis of a State-Space Based Approach to the Design of Hybrid Systems,” (Dinghao Wu and Jian Lü), *Journal of Nanjing University (Natural Sciences)*, **35**(5):564–572, 1999.
- [7] (in Chinese) “Software Interoperability: A Comparative Study of CORBA and Other Approaches,” (Junhua Ding, Huan Dong, Dinghao Wu, and Jian Lü), *Computer Research and Development*, **35**(7):577–583, 1998.
- [8] (in Chinese) “A State-Space Based Approach to the Design of Hybrid Systems,” (Dinghao Wu and Jian Lü), *Proceedings of the Seventh CCF National Conference of Young Computer Scientists (NCYCS 1998)*, China Computer Federation (CCF), Shanghai Sci-Tech Press. Shanghai, China, October 1998, 48–53.
- [9] “Two-Dimensional Dealiasing of Doppler Velocities,” (Guoqing Liu, Wenzhong Ge, Xueru Zhang, Dinghao Wu, and Ji Zhou), *Proceedings of the Twenty-seventh International Conference on Radar Meteorology*, American Meteorological Society. Vail, Colorado, October 9–13, 1995.

### **Patent**

- [10] “Data Race Detection Using Sequential Program Analysis,” (with Shaz Qadeer, Microsoft Corporation), US Patent US7316005. Filed on January 26, 2004. Issued on January 01, 2008.
- [11] “Detecting Data Race and Atomicity Violation via Typestate-Guided Static Analysis,” (Yue Yang, Anna Gringauze, Dinghao Wu, and Henning Rohde), US Patent Application 327545.01.

### **Theses**

- [12] “Interfacing Compilers, Proof Checkers, and Proofs for Foundational Proof-Carrying Code,” Ph.D. thesis, Department of Computer Science, Princeton University, 2005.
- [13] “A State-Space Based Approach to the Specification and Verification of Hybrid Systems and Its Axiomatic Basis,” Master’s thesis, Department of Computer Science, Nanjing University, 1999.
- [14] (in Chinese) “Computer Simulation of Free Turbulent Jets,” Senior thesis, Department of Chemical Engineering, Nanjing Institute of Chemical Technology, 1996.

## References

### **Andrew W. Appel, Professor**

Department of Computer Science  
Center for Information Technology Policy  
Princeton University  
Princeton, NJ 08540  
Email: [appel@cs.princeton.edu](mailto:appel@cs.princeton.edu)  
Tel: (609) 258-4627  
Fax: (609) 258-1771

### **Shaz Qadeer, Senior Researcher**

Software Reliability Research Group  
Microsoft Research  
One Microsoft Way  
Redmond, WA 98052  
Email: [qadeer@microsoft.com](mailto:qadeer@microsoft.com)  
Tel: (425) 707-9146  
Fax: (425) 936-7329

### **Sriram K. Rajamani, Principal Researcher & Research Manager**

Rigorous Software Engineering Group  
Microsoft Research India  
"Scientia" - 196/36 2nd Main  
Sadashivnagar, Bangalore 560 080  
India  
Email: [sriram@microsoft.com](mailto:sriram@microsoft.com)  
Tel: +91 (80) 5758-6000  
+91 (80) 5758-6005 (Direct)  
+91 9886095270 (Mobile)  
Fax: (425) 936-7329

### **Aaron Stump, Associate Professor**

Department of Computer Science  
The University of Iowa  
201F MacLean Hall  
Iowa City, IA 52242-1419  
Email: [astump@acm.org](mailto:astump@acm.org)  
Tel: (319)-384-0093

### **David Walker, Associate Professor**

Department of Computer Science  
Princeton University  
35 Olden Street  
Princeton, NJ 08540  
Email: [dpw@cs.princeton.edu](mailto:dpw@cs.princeton.edu)  
Tel: (609) 258-7654  
Fax: (609) 258-1771