

Zhong Shao

October 2011

- Address** Department of Computer Science
Yale University
51 Prospect Street
New Haven, CT 06520-8285, USA
Tel: +1 203 432 6828 Fax: +1 203 432 0593
Email: zhong.shao@yale.edu
URL: <http://www.cs.yale.edu/homes/shao>
- Interests** Programming languages and compilers, with a focus on language-based support for safety and security, certified system software, certified programming, certifying compilation, formal methods and proof automation, concurrency and coordination, and type systems.
- Education** Ph.D. in Computer Science, Princeton University, September 1994.
Thesis title: *Compiling Standard ML for efficient execution on modern machines*.
Advisor: Professor Andrew W. Appel.
- M.A. in Computer Science, Princeton University, May 1991.
- B.S. in Computer Science, University of Science and Technology of China, July 1988.
- Professional Experience** Yale University, Department of Computer Science, Assistant Professor, 1994–2000; Associate Professor, 2000–2003; Professor, since July 2003.
- USTC-Yale Joint Research Center for High-Confidence Software, Co-Director, since 2008.
- Microsoft Research, Redmond, WA. Summer 2008, Visiting Researcher.
- DoCoMo Communications Laboratories USA, Palo Alto, CA. December 2007– August 2008, Consultant.
- Bell Laboratories, Computing Sciences Research Center, Murray Hill, NJ, 1995–2001, Consultant. Worked on the Standard ML of New Jersey (SML/NJ) project.
- Xerox Palo Alto Research Center, Summer 1993, Research Intern for Dr. Hans Boehm and Dr. John Ellis. Developed a set of runtime optimizations for Boehm’s conservative garbage collector; built its interfaces in the GNU GCC and SRC Modula-3 compilers.
- Bell Laboratories, Computing Sciences Research Center, Murray Hill, NJ, Summer 1991, Research Intern for Dr. David MacQueen. Designed a new separate compilation system for Standard ML; developed tools and optimizations for the SML/NJ project.
- Princeton University, Department of Computer Science, 1989–1994, Research Assistant for Prof. Andrew W. Appel; Teaching Assistant for courses on systems programming and theory of algorithms.
- Chinese Academy of Science, Institute of Software, Beijing, China, 1988–1989. Research Assistant. Worked for Prof. C.S. Tang and Prof. Huimin Lin on algebraic specifications of abstract datatypes and semantics-based programming environments.

University of Science and Technology of China, Hefei, China, 1986–1988, Research Staff and Team Leader. Designed, developed, and commercialized a software system on educational management and timetable scheduling.

Grants

Making OS Kernels Crash-Proof by Design and Certification (with Bryan Ford), National Science Foundation Grant CNS-1065451, \$1,116,262. August 2011–July 2015.

Advanced Development of Certified OS Kernels (with Bryan Ford), Defense Advanced Research Projects Agency (DARPA), \$2,657,704, September 2010–September 2014.

Formal Reasoning about Concurrent Programs for Multicore and Multiprocessor Machines, National Science Foundation Grant CNS-0915888, \$500,000, September 2009–August 2012.

Combining Foundational and Lightweight Formal Methods to Build Certifiably Dependable Software, National Science Foundation Grant CNS-0910670, \$580,000, July 2009–June 2013.

Domain Specific Languages, Logics, and Proofs for Certified Software Design (with Paul Hudak), National Science Foundation Grant CCF-0811665, \$850,000 (REU supplement: \$19,238), July 2008–June 2011.

Microsoft Corporation Research Grant on Language and Compiler Support for Constructing Certified Systems Software, \$100,000, April 2008–June 2009.

Certified Runtime Code Manipulation, National Science Foundation Program on Cyber Trust, CCF-0716540, \$100,000, August 2007–July 2008.

Modular Development of Certified Concurrent Code, National Science Foundation Program on Cyber Trust, CCF-0524545, \$400,000, August 2005–July 2008.

Intel Corporation Research Grant, \$120,000, July 2004–June 2007.

Microsoft Corporation Research Grant, \$72,000, April 2004–June 2006.

High-Assurance Common Language Runtime (with Valery Trifonov), National Science Foundation Program on Trusted Computing (TC), CNS-0208618, \$400,000, August 2002–July 2005.

Microsoft Corporation Research Grant on Content and Curriculum, \$35,000. January 2003–December 2004.

Scaling Proof-Carrying Code to Production Compilers and Security Policies—Technology Transfer Extension (with Andrew Appel, Valery Trifonov, and David Walker), Defense Advanced Research Projects Agency (DARPA), \$1,346,386 (Yale FLINT component: \$636,154), June 2002–June 2004.

FLINT—A Mobile-Code Infrastructure for Advanced Languages, National Science Foundation Information Technology Research (ITR) Award, CCF-0081590, \$300,000, September 2000–August 2003.

Scaling Proof-Carrying Code to Production Compilers and Security Policies (with An-

drew Appel and Edward Felten), Defense Advanced Research Projects Agency (DARPA), \$2,224,772 (Yale FLINT component: \$1,058,951), June 1999–June 2002.

Typed Common Intermediate Format, National Science Foundation Program on Software Engineering and Languages, CCR-9901011, \$320,000, August 1999–July 2002.

Software Evolution using HOT Language Technology (with Paul Hudak and John Peterson), Defense Advanced Research Projects Agency (DARPA), \$698,837, August 1996–July 1999.

Foundations of HOT Languages and Software Evolution (with Paul Hudak), National Science Foundation Grant CCR-9633390, \$450,000, August 1996–July 1999.

Type-Directed Compilation, National Science Foundation Faculty Early CAREER Development Award CCR-9501624, \$105,000, June 1995–May 1998.

Software

Key developer of the Standard ML of New Jersey (SML/NJ) compiler since 1990. Main architect and implementor of several latest releases (including version 110). SML/NJ is a production-quality compiler for Standard ML 1997 currently used by thousands of students, researchers, and developers worldwide. Worked on the compiler front-end (type-checker, module elaborator, abstract syntax, semantic analysis), the middle-end (FLINT-based intermediate languages, representation analysis, FLINT optimizations, CPS-based intermediate languages, CPS conversion, CPS optimizations, space-efficient closure conversion), and the backend and the runtime system (generation of abstract machine code, callee-save registers).

Leader of the Yale FLINT group which previously developed the systems software (i.e., compiler infrastructure, runtime systems) for advanced type-safe languages such as ML, Java, and safe dialects of C. FLINT is the first production-quality type-preserving compiler infrastructure. The FLINT system is currently used inside the SML/NJ compiler and by several research groups working on type-directed compilation and proof-carrying code. The FLINT group is currently in the middle of developing a practical infrastructure for building large-scale certified systems software, focusing on the development of new program verification techniques and integrated programming and proof tools.

Publications *Refereed journal and highly selective, refereed conference papers:*

- [1] A. Stampoulis and Z. Shao. Static and User-Extensible Proof Checking. *Proceedings of the 39th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages (POPL12)*, Philadelphia, SC, pages (to appear), January 2012.
- [2] G. Tan, Z. Shao, X. Feng, and H. Cai. Weak Updates and Separation Logic. *New Generation Computing*, Volume 29, No.1, 2011, pages 1-29. Ohmsha, Ltd. and Springer.
- [3] Z. Shao. Certified Software. *Communications of ACM*, 53(12), pages 56–66, December 2010.
- [4] A. Stampoulis and Z. Shao. VeriML: Typed Computation of Logical Terms inside a Language with Effects. *Proceedings 2010 ACM SIGPLAN International Conference on Functional Programming (ICFP'10)*, Baltimore, Maryland, pages 333–344, September 2010.

- [5] M. Fu, Y. Li, X. Feng, Z. Shao, and Y. Zhang. Reasoning about Optimistic Concurrency using a Program Logic for History. *Proceedings of the 21st International Conference on Concurrency Theory (CONCUR'10)*, Paris, France, pages 388–402, August 2010.
- [6] R. Ferreira, X. Feng, and Z. Shao. Parameterized Memory Models and Concurrent Separation Logic. *Proceedings of the 19th European Symposium on Programming (ESOP'10)*, Paphos, Cyprus, pages 267–286, March 2010.
- [7] X. Feng, Z. Shao, Y. Dong, and Y. Guo. Certifying Low-Level Programs with Hardware Interrupts and Preemptive Threads. *Proceedings of the 2008 ACM SIGPLAN Conference on Programming Language Design and Implementation (PLDI'08)*, Tucson, AZ, pages 170–182, June 2008. An extended version of this paper appeared in *Journal of Automated Reasoning (Special Issue on Operating System Verification)*, 42(2-4):301-347, April 2009. Springer Science and Business Media B.V.2009.
- [8] A. McCreight, Z. Shao, C. Lin, and L. Li. A General Framework for Certifying Garbage Collectors and Their Mutators. *Proceedings of the 2007 ACM SIGPLAN Conference on Programming Language Design and Implementation (PLDI'07)*, San Diego, CA, pages 468–479, June 2007.
- [9] H. Cai, Z. Shao, and A. Vaynberg. Certified Self-Modifying Code. *Proceedings of the 2007 ACM SIGPLAN Conference on Programming Language Design and Implementation (PLDI'07)*, San Diego, CA, pages 66–77, June 2007.
- [10] X. Feng, R. Ferreira, and Z. Shao. On the Relationship Between Concurrent Separation Logic and Assume-Guarantee Reasoning. *Proceedings of the 16th European Symposium on Programming (ESOP'07)*, Braga, Portugal, March 2007. Published in Rocco De Nicola, editor, *Lecture Notes in Computer Science*, volume 4421, pages 173–188, Springer-Verlag, 2007.
- [11] X. Feng, Z. Shao, A. Vaynberg, S. Xiang, and Z. Ni. Modular Verification of Assembly Code with Stack-Based Control Abstractions, *Proceedings of the 2006 ACM SIGPLAN Conference on Programming Language Design and Implementation (PLDI'06)*, Ottawa, Canada, pages 401–414, June 2006.
- [12] Z. Ni and Z. Shao. Certified Assembly Programming with Embedded Code Pointers, *Proceedings of the 33rd ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages (POPL'06)*, Charleston, SC, pages 320–333, January 2006.
- [13] X. Feng and Z. Shao. Modular Verification of Concurrent Assembly Code with Dynamic Thread Creation and Termination, *Proceedings of the Tenth ACM SIGPLAN International Conference on Functional Programming (ICFP'05)*, Tallinn, Estonia, pages 254–267, September 2005.
- [14] Z. Shao, V. Trifonov, B. Saha, and N. Papaspyrou. A Type System for Certified Binaries. *ACM Transactions on Programming Languages and Systems (TOPLAS)*, 27(1), pages 1–45, January 2005.
- [15] D. Yu and Z. Shao. Verification of Safety Properties for Concurrent Assembly Code, *Proceedings of the Ninth ACM SIGPLAN International Conference on Functional Programming (ICFP'04)*, Snowbird, Utah, pages 175–188, September 2004.
- [16] D. Yu, N.A. Hamid, and Z. Shao. Building Certified Libraries for PCC: Dynamic Storage Allocation. In *Science of Computer Programming*, 50(1-3), pages 101-127, 2004.

- An early version of this paper appeared in *Proceedings of the 2003 European Symposium on Programming (ESOP'03)*, Warsaw, Poland, April 2003. Published in Pierpaolo Degano, editor, *Lecture Notes in Computer Science*, volume 2618, pages 363–379, Springer-Verlag, 2003.
- [17] B. Saha, V. Trifonov, and Z. Shao. Intensional Analysis of Quantified Types. *ACM Transactions on Programming Languages and Systems (TOPLAS)*, 25(2), pages 159–209, March 2003.
 - [18] S. Monnier and Z. Shao. Inlining as Staged Computation. *Journal of Functional Programming (JFP)*, 13(3), pages 647–676, May 2003.
 - [19] N.A. Hamid, Z. Shao, V. Trifonov, S. Monnier, and Z. Ni. A Syntactic Approach to Foundational Proof-Carrying Code. *Proceedings of the 17th IEEE Annual Symposium on Logic in Computer Science (LICS'02)*, Copenhagen, Denmark, pages 89–100, July 2002. An extended version of this paper appeared in *Journal of Automated Reasoning (JAR)*, 31(3-4), pages 191–229, October 2003.
 - [20] C. League, Z. Shao, and V. Trifonov. Type-Preserving Compilation of Featherweight Java. *ACM Transactions on Programming Languages and Systems (TOPLAS)*, 24(2), pages 112–152, March 2002.
 - [21] Z. Shao, B. Saha, V. Trifonov, and N. Papaspyrou. A Type System for Certified Binaries. *Proceedings of the 29th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages (POPL'02)*, Portland, OR, pages 217–232, January 2002.
 - [22] S. Monnier, B. Saha, and Z. Shao. Principled Scavenging. *Proceedings of the 2001 ACM SIGPLAN Conference on Programming Language Design and Implementation (PLDI'01)*, Snowbird, UT, pages 81–91, June 2001.
 - [23] V. Trifonov, B. Saha, and Z. Shao. Fully Reflexive Intensional Type Analysis. *Proceedings of the Fifth ACM SIGPLAN International Conference on Functional Programming (ICFP'00)*, Montreal, Canada, pages 82–93, September 2000.
 - [24] Z. Shao and A.W. Appel. Efficient and Safe-for-Space Closure Conversion. *ACM Transactions on Programming Languages and Systems (TOPLAS)*, 22(1), pages 129–161, January 2000.
 - [25] C. League, Z. Shao, and V. Trifonov. Representing Java Classes in a Typed Intermediate Language. *Proceedings of the Fourth ACM SIGPLAN International Conference on Functional Programming (ICFP'99)*, Paris, France, pages 183–196, September 1999.
 - [26] Z. Shao. Transparent Modules with Fully Syntactic Signatures. *Proceedings of the Fourth ACM SIGPLAN International Conference on Functional Programming (ICFP'99)*, Paris, France, pages 220–232, September 1999.
 - [27] Z. Shao, C. League, and S. Monnier. Implementing Typed Intermediate Languages. *Proceedings of the Third ACM SIGPLAN International Conference on Functional Programming (ICFP'98)*, Baltimore, MD, pages 313–323, September 1998.
 - [28] Z. Shao. Typed Cross-Module Compilation. *Proceedings of the Third ACM SIGPLAN International Conference on Functional Programming (ICFP'98)*, Baltimore, MD, pages 141–152, September 1998.

- [29] Z. Shao. Flexible Representation Analysis. *Proceedings of the Second ACM SIGPLAN International Conference on Functional Programming (ICFP'97)*, Amsterdam, The Netherlands, pages 85–98, June 1997.
- [30] A.W. Appel and Z. Shao. Empirical and Analytic Study of Stack vs. Heap Cost for Languages with Closures. *Journal of Functional Programming (JFP)*, 6(1), pages 47–74, January 1996.
- [31] Z. Shao and A.W. Appel. A Type-Based Compiler for Standard ML. *Proceedings of the 1995 ACM SIGPLAN Conference on Programming Language Design and Implementation (PLDI'95)*, La Jolla, California, pages 116–129, June 1995.
- [32] Z. Shao and A.W. Appel. Space Efficient Closure Representations. *Proceedings of the ACM SIGPLAN Conference on Lisp and Functional Programming (LFP'94)*, Orlando, FL, pages 150–161, June 1994.
- [33] Z. Shao, J.H. Reppy, and A.W. Appel. Unrolling Lists. *Proceedings of the ACM SIGPLAN Conference on Lisp and Functional Programming (LFP'94)*, Orlando, FL, pages 185–195, June 1994.
- [34] Z. Shao and A.W. Appel. Smartest Recompile. *Proceedings of the 20th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages (POPL'93)*, Charleston, SC, pages 439–450, January 1993.
- [35] A.W. Appel and Z. Shao. Callee-save Registers in Continuation-Passing Style. *Lisp and Symbolic Computation*, 5(3), pages 189–219, 1992.

Other refereed conference and workshop papers:

- [36] W. Wang, Z. Shao, X. Jiang, and Y. Guo. A Simple Model for Certifying Assembly Programs with First-Class Function Pointers. *Proc. 4th IEEE & IFIP International Symposium on Theoretical Aspects of Software Engineering (TASE'11)*, Xian, China, August 2011.
- [37] L. Gu, A. Vaynberg, B. Ford, Z. Shao, and D. Constanzo. CertiKOS: A Certified Kernel for Secure Cloud Computing. *Proc. 2nd ACM SIGOPS Asia-Pacific Workshop on Systems (APSys'11)*, Shanghai, China, July 2011.
- [38] G. Tan, Z. Shao, X. Feng, and H. Cai. Weak Updates and Separation Logic. *Proceedings of the 7th Asian Symposium on Programming Languages and Systems (APLAS'09)*, Seoul, Korea, December 2009. Published in *Lecture Notes in Computer Science*, volume 5904, pages 178–193, Springer-Verlag, 2009.
- [39] X. Feng, Z. Shao, Y. Guo, and Y. Dong. Combining Domain-Specific and Foundational Logics to Verify Complete Software Systems. *Proceedings of the 2nd IFIP Working Conference on Verified Software: Theories, Tools, and Experiments (VSTTE'08)*, Toronto, Canada, October 2008. Published in *Lecture Notes in Computer Science*, Springer-Verlag, 2008.
- [40] Z. Ni, D. Yu, and Z. Shao. Using XCAP to Certify Realistic System Code: Machine Context Management. *Proceedings of the 20th International Conference on the Applications of Higher Order Logic Theorem Proving (TPHOLs'07)*, Kaiserslautern, Germany, September 2007. Published in *Lecture Notes in Computer Science*, volume 4732, pages 189–206, Springer-Verlag, 2007.

- [41] C. Lin, A. McCreight, Z. Shao, Y. Chen, and Y. Guo. Foundational Typed Assembly Language with Certified Garbage Collection. *Proc. 1st IEEE & IFIP International Symposium on Theoretical Aspects of Software Engineering (TASE'07)*, Shanghai, China, pages 326–335, June 2007.
- [42] X. Feng, Z. Ni, Z. Shao, and Y. Guo. An Open Framework for Foundational Proof-Carrying Code. *Proceedings of the 2007 ACM SIGPLAN International Workshop on Types in Language Design and Implementation (TLDI'07)*, Nice, France, pages 67–78, January 2007.
- [43] N. Hamid and Z. Shao. Interfacing Hoare Logic and Type Systems for Foundational Proof-Carrying Code. *Proceedings of the 17th International Conference on the Applications of Higher Order Logic Theorem Proving (TPHOLs'04)*, Park City, Utah, September 2004. Published in Konrad Slind, editor, *Lecture Notes in Computer Science*, volume 3223, pages 118–135, Springer-Verlag, 2004.
- [44] C. League, Z. Shao, and V. Trifonov. Precision in Practice: A Type-Preserving Java Compiler. *Proceedings of the 12th International Conference on Compiler Construction (CC'03)*, Warsaw, Poland, April 2003. Published in Gorel Hedin, editor, *Lecture Notes in Computer Science*, volume 2622, pages 106–120, Springer-Verlag, 2003.
- [45] D. Yu, Z. Shao, and V. Trifonov. Supporting Binary Compatibility with Static Compilation. *Proceedings of the Second USENIX Java Virtual Machine Research and Technology Symposium (JVM'02)*, San Francisco, CA, pages 165–180, August 2002. *Winner of the Best Student Paper Award*.
- [46] D. Yu, V. Trifonov, and Z. Shao. Type-Preserving Compilation of Featherweight IL (Extended Abstract). *Proceedings of the 2002 International Workshop on Formal Techniques for Java-like Programs (FTfJP'02)*, June 2002.
- [47] C. League, V. Trifonov, and Z. Shao. Functional Java Bytecode. *Proceedings of the 2001 Workshop on Intermediate Representation Engineering for the Java Virtual Machine (IRE'01) at the 5th World Multi-conference on Systemics, Cybernetics, and Informatics*, Orlando, Florida, July 2001.
- [48] C. League, V. Trifonov, and Z. Shao. Type-Preserving Compilation of Featherweight Java. *Proceedings of the Eighth ACM SIGPLAN International Workshop on Foundations of Object-Oriented Languages (FOOL'01)*, London, UK, January 2001.
- [49] B. Saha, V. Trifonov, and Z. Shao. Fully Reflexive Intensional Type Analysis with Type Erasure Semantics. *Proceedings of the Third International Workshop on Types in Compilation (TIC'00)*, Montreal, Canada, September 2000.
- [50] V. Trifonov and Z. Shao. Safe and Principled Language Interoperation. *Proceedings of the 1999 European Symposium on Programming (ESOP'99)*, Amsterdam, The Netherlands, March 1999. Published in S. Doaitse Swierstra, editor, *Lecture Notes in Computer Science*, volume 1576, pages 128–146, Springer-Verlag, 1999.
- [51] B. Saha and Z. Shao. Optimal Type Lifting. *Proceedings of the Second International Workshop on Types in Compilation (TIC'98)*, Kyoto, Japan, March 1998. Published in Xavier Leroy and Astushi Ohori, editors, *Lecture Notes in Computer Science*, volume 1473, pages 156–177, Springer-Verlag, 1998.
- [52] Z. Shao and V. Trifonov. Type-Directed Continuation Allocation. *Proceedings of the Second International Workshop on Types in Compilation (TIC'98)*, Kyoto, Japan,

March 1998. Published in Xavier Leroy and Astushi Ohori, editors, *Lecture Notes in Computer Science*, volume 1473, pages 116–135, Springer-Verlag, 1998.

- [53] Z. Shao. Typed Common Intermediate Format. *Proceedings of the 1997 USENIX Conference on Domain-Specific Languages (DSL'97)*, Santa Barbara, CA, pages 89–102, October 1997.
- [54] Z. Shao. An Overview of the FLINT/ML Compiler. *Proceedings of the First International Workshop on Types in Compilation (TIC'97)*, Amsterdam, The Netherlands, June 1997.
- [55] H. Boehm and Z. Shao. Inferring Type Maps during Garbage Collection. *Proceedings of the OOPSLA'93 Workshop on Memory Management and Garbage Collection*, Washington, DC, September 1993.
- [56] Z. Shao. The Practical University Timetable Problem and its Timetabling Algorithm. *Proceedings of the First National Conference for Young Computer Scientists*, Harbin, China, August 1987.

Unrefereed papers and technical reports not published elsewhere:

- [57] S. Monnier and Z. Shao. Typed Regions. Technical Report YALEU DCS TR–1242, Dept. of Computer Science, Yale University, October 2002.
- [58] G. Collins and Z. Shao. Intensional Analysis of Higher-Kinded Recursive Types. Technical Report YALEU DCS TR–1240, Dept. of Computer Science, Yale University, October 2002.
- [59] D. Yu, V. Trifonov, and Z. Shao. Type-Preserving Compilation of Featherweight IL. Technical Report YALEU DCS TR–1228, Dept. of Computer Science, Yale University, April 2002.
- [60] A.W. Appel, Z. Shao, V. Trifonov, and D. Walker. High-Assurance Common Language Runtime. Technical Report YALEU DCS TR–1225, Dept. of Computer Science, Yale University, December 2001.
- [61] D. Teller and Z. Shao. Algorithm-Independent Framework for Verifying Integer Constraints. Technical Report YALEU DCS TR–1195, Dept. of Computer Science, Yale University, June 2000.
- [62] A.W. Appel, E. Felten, and Z. Shao. Scaling Proof-Carrying Code to Production Compilers and Security Policies. Technical Report YALEU DCS TR–1182, Dept. of Computer Science, Yale University, January 1999.
- [63] The ML2000 Working Group. Principles and a Preliminary Design for ML2000. March 1999.
- [64] S. Monnier, M. Blume, and Z. Shao. Cross-Function Inlining in FLINT. Technical Report YALEU DCS TR–1189, Dept. of Computer Science, Yale University, March 1999.
- [65] C. League, Z. Shao, and V. Trifonov. Encoding Java Classes in a Typed Intermediate Language. Technical Report YALEU DCS TR–1173, Dept. of Computer Science, Yale University, December 1998.

- [66] S. Monnier and Z. Shao. The FLINT Optimizer. Technical Report YALEU DCS TR-1172, Dept. of Computer Science, Yale University, December 1998.
- [67] C. League and Z. Shao. Formal Semantics of the FLINT Intermediate Language. Technical Report YALEU DCS TR-1171, Dept. of Computer Science, Yale University, May 1998.
- [68] Z. Shao. Parameterized Signatures and Higher-Order Modules. Technical Report YALEU DCS TR-1161, Dept. of Computer Science, Yale University, August 1998.
- [69] Z. Shao. Compiling Standard ML for Efficient Execution on Modern Machines. Ph.D. Thesis. Technical Report CS-TR-475-94, Dept. of Computer Science, Princeton University, September 1994.
- [70] Z. Shao. A Practical University Timetabling System. Zhong Shao. Bachelor's Thesis (in Chinese), University of Science and Technology of China, June 1988.

Professional Activities

- Member of External Review Committee, *Thirty-ninth ACM Symposium on Principles of Programming Languages (POPL'12)*, Philadelphia, PA, January 2012.
- Program Co-Chair, *First International Conference on Certified Programs and Proofs (CPP)*, 2011.
- Program Co-Chair, *2011 International Workshop on Syntax and Semantics of Low Level Languages (LOLA)*, 2011.
- Member of Program Committee, *Third International Conference on Verified Software: Theories, Tools, and Experiments (VSTTE'10)*, Edinburgh, Scotland, August 2010.
- Member of Program Committee, *Fifth International Workshop on Systems Software Verification (SSV'10)*, Vancouver, Canada, October 2010.
- Member of Program Committee, *Tenth International Symposium on Functional and Logic Programming (FLOPS'10)*, Sendai, Japan, April 2010.
- Member of Program Committee, *Fifth ACM SIGPLAN Workshop on Types in Language Design and Implementation (TLDI'10)*, Madrid, Spain, January 2010.
- Member of Program Committee, *Fourth International Workshop on Systems Software Verification (SSV'09)*, Aachen, Germany, June 2009.
- Chair of Steering Committee, *ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages (POPL)*, 2009-2010.
- General Chair, *Thirty-sixth ACM Symposium on Principles of Programming Languages (POPL'09)*, January 2009.
- Member of Program Committee, *Third International Workshop on Systems Software Verification (SSV'08)*, Sydney, Australia, February 2008.
- Member of Program Committee, *Thirty-fifth ACM Symposium on Principles of Programming Languages (POPL'08)*, San Francisco, CA, January 2008.

Member of Editorial Board, *Journal of Computing Science and Engineering (JCSE)*, 2007–present.

Program Chair, *Fifth Asian Symposium on Programming Languages and Systems (APLAS'07)*, Singapore, November 2007.

Member of Program Committee, *First IEEE and IFIP International Symposium on Theoretical Aspects of Software Engineering (TASE'07)*, Shanghai, China, June 2007.

Member of Program Committee, *Eighth International Symposium on Trends in Functional Programming (TFP'07)*, New York, April 2007.

Member of Program Committee, *Sixteenth International Conference on Compiler Construction (CC'07)*, Braga, Portugal, March 2007.

Member of Program Committee, *Fourth Asian Symposium on Programming Languages and Systems (APLAS'06)*, Sydney, Australia, November 2006.

Member of Program Committee, *Fourth International Symposium on Automated Technology for Verification and Analysis (ATVA'06)*, Beijing, China, October 2006.

Member of Editorial Board, *Journal of Computer Science and Technology (JCST)*, 2006–present.

Member of Program Committee, *IJCAR Workshop on Programming Languages meets Program Verification (PLPV'06)*, Seattle, Washington, August 2006.

Member of Program Committee, *Seventh International Symposium on Trends in Functional Programming (TFP'06)*, Nottingham, UK, April, 2006.

Panel Organizer and Moderator, *The Future of Programming*, Yale Computer Science 35th Anniversary and Alumni Conference: Computer Science in the New Information Society, November 2005.

Member of Program Committee, *2005 ACM SIGPLAN Workshop on ML*, Tallinn, Estonia, September 2005.

Invited Speaker at the New England Programming Languages and Systems Symposium Series (NEPLS), Boston, MA, February 2005.

Member of Program Committee, *Thirty-second ACM Symposium on Principles of Programming Languages (POPL'05)*, Long Beach, CA, January 2005.

Invited Speaker on “The Essence of Proof-Carrying Code” at the *TYPES 2004 Conference*, Jouy-en-Josas, France, December 2004.

Member of Steering Committee, *ACM SIGPLAN International Conference on Functional Programming (ICFP)*, 2004–2006.

Member of Advisory Board, Asian Association for Foundation of Software, 2003–present.

Member of Program Committee, *First Asian Symposium on Programming Languages and Systems (APLAS'03)*, Beijing, China, November 2003.

Member of Program Committee, *2003 ACM Workshop on Survivable and Self-Regenerative Systems (SSRS'03)*, Fairfax, VA, October 2003.

Member of Program Committee, *Eighth ACM SIGPLAN International Conference on Functional Programming (ICFP'03)*, Uppsala, Sweden, August 2003.

Member of Workshop Selection Committee, *2003 Conferences and Workshops on Principles, Logics, and Implementations of High-Level Programming Languages (PLI'03)*, Uppsala, Sweden, August 2003.

General Chair, *ACM SIGPLAN Workshop on Types in Language Design and Implementation (TLDI'03)*, New Orleans, LA, January 2003.

Member of Program Committee, *First International Workshop on Types in Programming (TIP'02)*, Dagstuhl, Germany, July 2002.

Member of Steering Committee, *ACM SIGPLAN Workshops on Types in Language Design and Implementation*, March 2002–present.

Invited Speaker, *Intel Research Forum on Language-Based Security*, Santa Clara, CA, January 2002.

Invited Speaker, *First International Workshop on Multi-Language Infrastructure and Interoperability (BABEL'01)*, Firenze, Italy, September 2001.

Invited Speaker, *Dagstuhl Seminar No. 01341 on Dependent Type Theory meets Practical Programming*, Dagstuhl, Germany, August 2001.

Members at Large, *ACM SIGPLAN Executive Committee*, 2001–2005.

Invited Tutorial on Type-Based Certifying Compilation, *ACM SIGPLAN Conference on Programming Language Design and Implementation (PLDI'01)*, Snowbird, UT, June 2001.

Member of Editorial Board, *Journal of Functional Programming*, 2001–2010.

Moderator, *Programming Languages: Theory vs. Practice*, Alan J. Perlis Symposium, Sponsored by Department of Computer Science, Yale University, April 2000.

Panelist, *Typed Intermediate Languages for Compiling Object-Oriented Languages*, Seventh International Workshop on Foundations of Object-Oriented Languages, Boston, MA, January 2000.

Member of Program Committee, *ACM SIGPLAN Conference on Programming Language Design and Implementation (PLDI'99)*, Atlanta, GA, May 1999.

Member of Program Committee, *Second ACM SIGPLAN International Workshop on Types in Compilation (TIC'98)*, Kyoto, Japan, March 1998.

Member of Program Committee, *Twenty-third ACM Symposium on Principles of Programming Languages (POPL'96)*, St. Petersburg, FL, January 1996.

Member of the ML2000 Working Group, 1993–2000.

Member of various review panels for National Science Foundation, 1996–present.

Reviewer for *Journal of Functional Programming*, *Software: Practice and Experience*, *ACM Transactions on Programming Languages and Systems*, *Journal of Information and Computation*, *ACM Transactions on Software Engineering and Methodology*, and a number of conferences on programming languages and compilers. Reviewer for *Cambridge University Press*, *Prentice Hall*, *McGraw Hill*, *Addison Wesley*, *Thomson* in the area of introductory programming, compilers, and programming languages. 1993–present.

Member of ACM, USENIX, and IEEE Computer Society, 1990–present

Teaching Experience

CS112 Introduction to Programming (four semesters).

CS210 A Second Course in Programming (two semesters).

CS421/521 Compilers and Interpreters (eleven semesters).

CS422/522 Operating Systems (three semesters).

CS428/528 Language-Based Security (three semesters).

CS430/530 Formal Semantics (four semesters).

CS535 Advanced Topics in Modern Compiler Implementation (one semester).

Graduate seminar on functional languages (two semesters).

Graduate seminar on secure internet programming (one semester).

Graduate seminar on understanding Java virtual machine (two semesters).

Students

Post-Doctoral Research Associate: Valery Trifonov (1997–2000).

Post-Doctoral Research Associate: Nikolaos Papaspyrou (2000–2001).

Former Ph.D. students:

- Bratin Saha, Ph.D.(2002). Thesis title: *A Type System for Certified Runtime Type Analysis*. Current Employment: Intel Research Labs, Santa Clara, CA.
- Christopher League, Ph.D.(2002). Thesis title: *A Type-Preserving Compiler Infrastructure*. Current Employment: Associate Professor, Long Island University.
- Stefan Monnier, Ph.D.(2003). Thesis title: *Principled Compilation and Scavenging*. Current Employment: Associate Professor, University of Montreal.
- Dachuan Yu (2004). Thesis title: *Safety Verification of Low-Level Code*. Current Employment: Orange Labs, France Telecom.

- Nadeem A. Hamid (2004). Thesis title: *A Syntact Approach to Foundational Proof-Carrying Code*. Current Employment: Associate Professor, Berry College.
- Zhaozhong Ni (2006). Thesis title: *Modular Machine Code Verification*. Current Employment: 3PAR Inc.
- Xinyu Feng (2007). Thesis title: *An Open Framework for Certified System Software*. Current Employment: Professor, University of Science and Technology of China.
- Hongxu Cai (2008). Thesis title: *Logic-based Verification of General Machine Code*. Current Employment: Google Inc.
- Andrew McCreight (2008). Thesis title: *The Mechanized Verification of Garbage Collector Implementations*. Current Employment: Mozilla.
- Rodrigo Ferreira (2010). Thesis title: *Memory Consistency and Program Verification*. Current Employment: Brazil.

Current Ph.D. students:

- Alexander Vaynberg (2004–present). Research interest: *Programming Languages; Certified Operating Systems*.
- Antonis Stampoulis (2006–present). Research interest: *Programming Languages; Proof Assistants*.
- David Costanzo (2008–present). Research interest: *Programming Languages; Separation Logic*.
- Shu-Chun Weng (2009–present). Research interest: *Programming Languages; Security*.

Undergraduate students (advising their senior projects): Chris Volkert (1995), Jonathan Traupman (1996), Lujo Bauer (1997), Ben Zhao (1997), Alex Hehmeyer (1997), Kenny Wolf (1997), Jesse Heitler (1997), Bret Martin (1997), David Auerbach (1998), Neil Inala (1998), John Richter (1999), Benjamin Christen (2000), John Garvin (2000–2001), Yichen Xie (2000), Daniel Dormont (2001), John Starks (2007), Alexander Thomson (2008), Aarlo Stone-Fish (2009), and Eric Love (2011).

Research interns and visitors: Rudi Seitz (1996), Neil Inala (1996), Sukyoung Ryu (1999), Oukseh Lee (1999), David Teller (2000), Yichen Xie (2000–2001), John Garvin (2000–2001), Yuan Dong (2007–2008), Wei Wang (2008–2010), Ming Fu (2009–2010), Yong Li (2009–2010), Guillaume Claret (2010), Xinyu Jiang (2010–2011), Yu Zhang (2010–2011), Xinyu Feng (2011), Zhong Zhuang (2010–2012), Haozhong Zhang (2011–2012), and Jin-jiang Lei (2011–2012).

Member of the Ph.D. thesis committee: Jan-Jan Wu (1995), Satish Pai (1996), Rajiv Mirani (1996), Kevin Lynch (1996), Sheng Liang (1997), Chih-Ping Chen (1999), Martin Sulzmann (1999), Mark Tullsen (2001), Bratin Saha (2002), Christopher League (2002), Zhanyong Wan (2002), Stefan Monnier (2003), Juan Chen (2004), Anthony Courtney (2004), Dachuan Yu (2004), Nadeem A. Hamid (2004), Zhaozhong Ni (2006), Xinyu Feng (2007), Liwen Huang (2008), Andrew McCreight (2008), Adam Poswalski (2008), Jeffrey Sarnat (2009), Rodrigo Ferreira (2010), Paul Liu (2011), and Jan Hoffmann (2011).

**University
Activities**

Director of Undergraduate Studies, Yale Computer Science, 2003–2006.

Acting Chair, Graduate Admission Committee, Yale Computer Science, 2001.

Member, Graduate Admission Committee, Yale Computer Science, 1995–1997, 2000, 2008–2011.

Organizer, Weekly Systems Seminar (SPAM), Yale Computer Science, 1994–1996.
Organizer, Yale Computer Science Alan J. Perlis Symposium, 2000–2001.
Member, Ph.D. Comprehensive Exam Committee, Yale Computer Science, 1995–2001.
Member, Computing Committee, Yale Computer Science, 2003–2005.
Member, Financial Committee, Yale Computer Science, 2005–2006.
Member, Faculty Recruiting Committee, Yale Computer Science, 2005–present.
Member, Teaching and Curriculum Committee, Yale Computer Science, 1996–2006.
Member, Curriculum 200X Committee, Yale Computer Science, 2001–2003.
Member, Library Committee, Yale Computer Science, 1996–2001.
First-year Graduate Student Coordinator, Yale Computer Science, 1997–2000.
Fellow, Silliman College, Yale University, 1995–present.
Freshman Advisor, Silliman College, Yale University, 1995–1999, 2004.
Sophomore Advisor, Yale Computer Science, 1999–present.