

Fang Yu

PhD Candidate
Department of Computer Science
University of California
2162 Frank Hall
Santa Barbara, CA 93106

Home Address:
713 Gayley Walk Apt 104
Goleta, CA 93117
Phone: 310 3212072
yuf at cs.ucsb.edu
<http://www.cs.ucsb.edu/~yuf>

OBJECTIVE ◇ A full time position for software verification

EDUCATION ◇ University of California at Santa Barbara, CA, U.S.
PhD Student, Department of Computer Science, Fall 2005-Present.
GPA: 3.97/40 GPA Units/ 161 CS Units

◇ National Taiwan University, Taipei, Taiwan
Master of Business Administration in Information Management, 1998-2000.
GPA: 4.00/42 GPA Units, Rank: 1/21
Thesis: *Automatic Multi-target Negotiation in an Option-based Electronic Marketplace*.
Advisor: Prof. Seng-Cho T. Chou
Bachelor of Business Administration in Information Management, 1994-1998.
Last 2yrs GPA: 3.96/79 Units, Overall GPA: 3.52/173 Units.

WORK EXPERIENCE ◇ Fall 2006-Present: Research Assistant under the supervision of Prof. Tefvik Bultan, Dept. of Computer Science, University of California at Santa Barbara.

◇ Summer 2008: Intern, NEC Laboratories America, Inc. Princeton, NJ. Project: Thread-sensitive Concurrent Data Flow analysis, supervised by Chao Wang.

◇ Summer 2007: Intern, NEC Laboratories America, Inc. Princeton, NJ. Project: Modular Verification of Web Service Composition, supervised by Chao Wang.

◇ Fall 2005-Spring 2006: Teaching Assistant, Dept. of Computer Science, University of California at Santa Barbara.

◇ 2001–2005: Research Assistant, Institute of Information Science, Academia Sinica

◇ Spring 2004, 2005: Lecturer, Taiwan Computer Olympiad Representatives.

RESEARCH INTERESTS ◇ String Analysis
◇ Model Checking
◇ Software/Hardware Verification

AWARDS AND HONORS ◇ 2008-2009: UCSB Deans Fellowship
◇ 2009: ETAPS Scholarship
◇ 2008: Sigsoft CAPS for FSE Travel Support
◇ 2008: Adobe Best Paper Award, the 3rd UCSB Graduate Student Workshop on Computing
◇ 2004: Best Paper Nominee, the 13th World Wide Web Conference
◇ 2000: Graduate first place from National Taiwan University
◇ 1995-97: Presidential Award, National Taiwan University

PAPERS AT REFERRED CONFERENCES ◇ *Generating Vulnerability Signatures for String Manipulating Programs Using Automata-based Forward and Backward Symbolic Analyses*
Fang Yu, Muath Alkhalaf, and Tefvik Bultan.
Short paper. Accepted for Publication in the 24th IEEE/ACM International Conference on Automated Software Engineering (ASE 2009).

- ◇ *Symbolic String Verification: Combining String Analysis and Size Analysis*
Fang Yu, Tevfik Bultan, and Oscar H. Ibarra.
In Proceedings of the 15th International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS 2009), LNCS 5505, pages 322-336, York, UK, Mar. 2009.
- ◇ *Modular Verification of Web Services Using Efficient Symbolic Encoding and Summarization*
Fang Yu, Chao Wang, Aarti Gupta, and Tevfik Bultan.
In Proceedings of the Sixteenth ACM SIGSOFT Symposium on Foundations of Software Engineering (SIGSOFT 2008/FSE 16), pages 192-202, Atlanta, GA, Nov. 2008.
- ◇ *Symbolic String Verification: An Automata-based Approach*
Fang Yu, Tevfik Bultan, Marco Cova, Oscar H. Ibarra.
In Proceedings of the 15th International SPIN Workshop on Model Checking of Software (SPIN 2008), LNCS 5156, pages 306-324, Los Angeles, CA, August 2008.
- ◇ *Automated Size Analysis for OCL*
Fang Yu, Tevfik Bultan, Erik Peterson.
In Proceedings of the 6th joint meeting of the European Software Engineering Conference and the ACM SIGSOFT Symposium on the Foundations of Software Engineering (ESEC/FSE 2007). pp. 331-340, Dubrovnik, Croatia, Sep. 2007.
- ◇ *On Spiking Neural P Systems and Partially Blind Counter Machines*
Oscar H. Ibarra, Sara Woodworth, Fang Yu, Andri Paun.
In Proceedings of the 5th International Conference on Unconventional Computation (UC 2006), York, UK, Sep. 2006.
- ◇ *Efficient Exact Spare Allocation via Boolean Satisfiability*
Fang Yu, Chung-Hung Tsai, Yaw-Wen Huang, Hung-Yau Lin, Der-Tsai Lee, Sy-yen Kuo.
In: Proceedings of the 20th IEEE International Symposium on Defect and Fault Tolerance in VLSI Systems (DFT 2005), pages 361-370, Monterey, CA, Oct. 2005.
- ◇ *Toward Unbounded Model Checking for Region Automata.*
Fang Yu and Bow-Yaw Wang.
In: Proceedings of the 2nd International Symposium on Automated Technology for Verification and Analysis (ATVA 2004), LNCS 3299, pages 20-33, Taipei, Taiwan, Oct 2004.
- ◇ *Bounded Model Checking for Region Automata.*
Fang Yu, Bow-Yaw Wang and Yaw-Wen Huang.
In: Proceedings of the Joint Conference on Formal Modelling and Analysis of Timed Systems and Formal Techniques in Real-Time and Fault Tolerant System (FORMATS-FTRTFT 2004), LNCS 3253, pages 246-262, Grenoble, France, Sep 2004.
- ◇ *Verifying Web Applications Using Bounded Model Checking.*
Yao-Wen Huang, Fang Yu, Christian Hang, Chung-Hung Tsai, Der-Tsai Lee, Sy-Yen Kuo.
In: Proceedings of the 2004 International Conference on Dependable Systems and Networks (DSN 2004), pages 199-208, Florence, Italy, Jun 2004.
- ◇ *Securing Web Application Code by Static Analysis and Runtime Protection.*
Yao-Wen Huang, Fang Yu, Christian Hang, Chung-Hung Tsai, Der-Tsai Lee, Sy-Yen Kuo.
In: Proceedings of the Thirteenth International World Wide Web Conference (WWW 2004), pages 40-52, New York, May 2004.
Best Paper Nominee.
- ◇ *Numerical Coverage Estimation for the Symbolic Simulation of Real-Time Systems.*
Farn Wang, Geng-Dian Huang, and Fang Yu.
In: Proceedings of the 23rd IFIP International Conference on Formal Techniques for Networked and Distributed Systems (FORTE 2003), LNCS 2767, Berlin, Sept.-Oct. 2003.
- ◇ *TCTL Inevitability Analysis of Dense-time Systems.*
Farn Wang, Geng-Dian Huang, and Fang Yu.

- In: Proceedings of the 8th International Conference on Implementation and Application of Automata (CIAA 2003), LNCS 2759, July 2003.
- ◇ *OVL Assertion Checking of Embedded Software with Dense-Time Semantics.*
Farn Wang and Fang Yu.
In: Proceedings of the 9th International Conference on Real-Time and Embedded Computing Systems and Applications (RTCSA 2003), LNCS 2968, February 2003.
 - ◇ *Symbolic Simulation of Real-Time Concurrent Systems.*
Farn Wang, Geng-Dian Huang, and Fang Yu.
In: Proceedings of the 9th International Conference on Real-Time and Embedded Computing Systems and Applications (RTCSA 2003), LNCS 2968, February 2003.
- PAPERS IN REFERRED JOURNALS
- ◇ *On Spiking Neural P Systems and Partially Blind Counter Machines*
Oscar H. Ibarra, Sara Woodworth, Fang Yu, Andri Paun.
Natural Computing, Springer Netherlands, ISSN:1567-7818 (Print) 1572-9796 (Online), May 2007.
 - ◇ *SAT-based Model Checking for Region Automata*
Fang Yu and Bow-Yaw Wang.
The International Journal of Foundations of Computer Science(IJFCS), Vol. 17, No. 4, pp. 775-796, August 2006.
 - ◇ *TCTL Inevitability Analysis of Dense-time Systems: from Theory to Engineering*
Farn Wang, Geng-Dian Huang and Fang Yu.
IEEE Transactions on Software Engineering, Vol. 32, No. 7, pp. 510-526. July 2006. ISSN: 0098-5589 2006.
 - ◇ *BDD-based Safety Analysis of Concurrent Software with Pointer Data Structures using Graph Automorphism Symmetry Reduction.*
Farn Wang, K. Schmidt, Fang Yu, Geng-Dian Huang, Bow-Yaw Wang.
IEEE Transactions on Software Engineering. Vol. 30, No. 6, pp. 403-417, Jun 2004.
 - ◇ *Symbolic Simulation of Industrial Real-Time and Embedded Systems - Experiments with the Bluetooth baseband communication protocol.*
Farn Wang, Geng-Dian Huang, Fang Yu.
Journal of Embedded Computing (JEC), Cambridge International Science Publishing, Vol. 1, No. 1, 2004.
- SHORT PAPERS AT REFERRED WORKSHOPS
- ◇ *Symbolic Encoding of String Lengths*
Fang Yu, Tevfik Bultan and Oscar H. Ibarra.
In Proceedings of the 3rd UCSB Graduate Student Workshop on Computing, Oct. 2008. (Best Paper Award)
 - ◇ *Automated Size Analysis of Object-oriented Systems*
Fang Yu and Tevfik Bultan.
In Proceedings of the 2nd UCSB Graduate Student Workshop on Computing, Sep. 2007.
- PATENT
- ◇ *Modular Verification of Web Services Using Efficient Symbolic Encoding and Summarization*
Chao Wang, Fang Yu, Aarti Gupta.
US Patent, Pending, Filed on Mar. 3, 2008, No. 61/033126.
 - ◇ *Systems and Methods for Securing Web Application Code*
Yao-Wen Huang, Fang Yu, Christian Hang, Chung-Hung Tsai, Der-Tsai Lee, Sy-Yen Kuo.
US Patent, Application, No. 20070074188, Mar. 2007.
- PUBLIC TALKS
- ◇ Oct. 2009: Proposal Talk, UCSB
Automatic Verification of String Manipulating Programs
 - ◇ Mar. 2009: Presentation in ETAPS/TACAS
Symbolic String Verification: Combining String Analysis and Size Analysis

- ◇ Nov. 2008: Presentation in SIGSOFT/FSE
Modular Verification of Web Services Using Efficient Symbolic Encoding and Summarization
- ◇ Oct. 2008: Presentation in GSWC (Best Paper Award)
Symbolic Encoding of String Lengths
- ◇ Aug. 2008: Presentation in SPIN
Symbolic String Verification: An Automata-based Approach
- ◇ Sep. 2007: Presentation in FSE
Automated Size Analysis for OCL.
- ◇ Jan. 2007: Major Area Exam, UCSB
Software Model Checking during Design and Implementation
Committee: Prof. Tevfik Bultan (Chair), Prof. Oscar H. Ibarra, Prof. Richard Kemmerer
- ◇ Oct. 2005: Presentation in DFT
Efficient Exact Spare Allocation via Boolean Satisfiability.
- ◇ Nov. 2004: Presentation in ATVA
Toward Unbounded Model Checking for Region Automata.
- ◇ Sep. 2004: presentation in FORMATS-FTRTFT
Bounded Model Checking for Region Automata.
- ◇ Jun. 2004: Presentation in DSN
Verifying Web Applications Using Bounded Model Checking.
- ◇ May 2004: Presentation in WWW (Best Paper Nominee)
Securing Web Application Code by Static Analysis and Runtime Protection.
- ◇ Feb. 2003: Presentation in RTCSA
OVL Assertion Checking of Embedded Software with Dense-Time Semantics.

RESEARCH
PROJECTS
AND TOOLS

- ◇ 2007 Fall-Present: String Analysis
Supervisor: Prof. Tevfik Bultan
Collaborators: Muath Alkhalaf and Marco Cova
String analysis is a static analysis technique that determines the string values that a variable can hold at specific points in a program. We develop an automata-based string analyzer, called Stranger, to detect and prevent string related vulnerabilities, e.g., XSS and SQLI, in web applications. Stranger combines forward and backward symbolic reachability analyses and generates string-based vulnerability signatures, i.e., a characterization that includes all malicious inputs that can be used to generate attacks. Stranger takes advantage on symbolic representation of automata, which allows the practical handling of automata on very large alphabets. Stranger also incorporates various novel approximation techniques and targets on proving the correctness of secured web applications efficiently. We later extend this automata-based approach to verify systems having both string and integer variables. By exchanging length information between string and arithmetic automata, we improve precision of both string and size analysis. Recently, we investigate the essence of string systems, and characterize the decidability of reachability analysis on various string systems. (SPIN 2008, TACAS 2009, ASE 2009)
- ◇ 2008 Summer: Thread-sensitive Concurrent Data Flow Analysis
Supervisor: Dr. Chao Wang
We propose a thread-sensitive concurrent data flow analysis using static single assignments, of which state propagation follows causality consistency. We apply our technique to perform precise constant propagation/code elimination on concurrent C programs, and reduce costs on verifying those programs.
- ◇ 2007 Summer: Scalable Verification of Service Composition
Supervisor: Dr. Chao Wang
We propose a novel method for modular verification of BPEL service composition. We first

- derive pre and post conditions for well defined web services based on infinite state model checking techniques. The derived pre and post conditions can be collected and served as the summarization of web services. Modular verification, by composing the summarization of external invocations, can then be applied to achieve scalable verification. (FSE 2008)
- ◇ 2006 Fall-2007 Winter: Size Analysis
Supervisor: Prof. Tevfik Bultan
 Collaborator: Erik Peterson
 We aim to verify specifications of object oriented systems based on infinite state model checking techniques. We target on object constraint language and propose size abstraction and size analysis. We conducted a case study on the OCL specifications of Java Card APIs. The experiments indicate our abstraction is precise enough to verify/falsify target systems, while coarse enough to perform complex model checking techniques efficiently. (FSE 2007)
 - ◇ 2006: Characterizing Spiking Neural P Systems
Supervisors: Prof. Oscar H. Ibarra
 Collaborators: Sara Woodworth and Andri Paun
 Neurons are arguably one of the most interesting cell-types in the human body. A large number of neurons working in a cooperative manner are able to perform tasks that are not yet matched by the tools we can build with our current technology. Spiking Neuron P-systems(SNPs) incorporate ideas from spiking neurons into membrane computing. In this project, we give characterizations of sets definable by partially blind multicounter machines in terms of k -output SNPs operating in a sequential mode. (UC 2006, NC 2008)
 - ◇ 2004-2005: Spare Allocation
Supervisors: Prof. Der-Tsai Lee and Prof. Sy-Yen Kuo
 Collaborators: Yaw-Wen Huang and Chung-Hung Tsai
 Fabricating large memory and processor arrays is subject to physical failures resulting in yield degradation. The strategy of incorporating spare rows and columns to obtain reasonable production yields was first proposed in the 1970s, and continues to serve as an important role in recent VLSI developments. Since the spare allocation problem (SAP) is NP-complete but requires solving during fabrication, an efficient exact spare allocation algorithm has great value. In this project, we proposed a novel Boolean encoding to reduce exact SAP to the satisfiability problem, so that we can leverage the capability of modern SAT solvers. (DFT 2005)
 - ◇ 2002-2005: Web Security (WebSARRI)
Supervisors: Prof. Der-Tsai Lee and Prof. Sy-Yen Kuo
 Collaborators: Yaw-Wen Huang, Christian Hang, and Chung-Hung Tsai
WebSSARI, a joint project between Academia Sinica and National Taiwan University, stands for Web application security via Static Analysis and Runtime Inspection. Viewing Web application vulnerabilities as a secure information flow problem, we created a lattice-based static analysis algorithm derived from type systems and tpestate. During the analysis, sections of code considered vulnerable are instrumented with runtime guards, thus securing Web applications in the absence of user intervention. Soundness, i.e no false negative, is achieved by applying formal methods including tpestate checking and bounded model checking. I worked on designing and developing core checkers including: (1) An light-weight Type Checker (WWW 2004), and (2) A heavy-weight Bounded Model Checker (DSN 2004).
 - ◇ 2003-2005: SAT-based Model Checking(x BMC)
Supervisor: Dr. Bow-Yaw Wang
 We take advantage on SAT-solvers' capability to support formal verification of discrete/real-time systems. Our contribution consists of expanding SAT-based model checking techniques from verifying discrete systems to dense-time systems, as well as from bounded to unbounded capabilities (FORMATS-FTRTFT 2004, ATVA 2004, IJFCS 2006).
 - ◇ 2002-2004: TCTL Model Checking (RED 4.0)
Supervisor: Prof. Farn Wang

Collaborator: Geng-Dian Huang

I was involved in designing and developing *RED 4.0* on top of *RED*, the full Timed-CTL symbolic model checker initiated by Prof. Farn Wang in 1996. *RED 4.0* enhanced *RED* in the following directions: (1) Symbolic Simulation (RTCSA 2003), (2) Numerical Coverage Estimation (FORTE 2003), (3) Greatest Fixpoint Computation (CIAA 2003, IEEE TSE 2006), and (4) Symmetric Analysis with Pointer Data Structure (IEEE TSE 2004).

◇ 2001-2002: Optimized Translation (*timeC*)

Supervisor: Prof. Farn Wang

timeC is a C-like language that combines basic C statements with timed statements and OVL (Open Verification Library) assertions. I developed an optimized translator that automatically translates *timeC*/OVL assertions to timed automata/TCTL formula, which can work with *RED* to verify systems specified in *timeC*. (RTCSA 2003).

REFERENCES

Prof. Tevfik Bultan

Professor, the Department of Computer Science, University of California, Santa Barbara
bultan at cs.ucsb.edu

Prof. Oscar H. Ibarra

IEEE Fellow, ACM Fellow, AAA Fellow

Professor, the Department of Computer Science, University of California, Santa Barbara
ibarra at cs.ucsb.edu

Dr. Chao Wang

Research Staff Member, NEC Laboratories America
chaowang at nec-labs.com

Prof. Farn Wang

Professor, the Department of Electrical Engineering, National Taiwan University
farn at cc.ee.ntu.edu.tw

Dr. Bow-Yaw Wang

Associate Research Fellow, the Institute of Information Science, Academia Sinica
bywang at iis.sinica.edu.tw