

Educational Background

Ph.D.	Computer Science	Stevens Institute of Technology	Jan. 2010	GPA 3.75
M.S.	Computer Science	SUNY Institute of Technology	Dec. 2004	GPA 3.58
B.S.	Computer Science	Clarkson University	May 1991	

Employment History

Employer	Period of Time	Title
SUNY Institute of Technology	2008-2009	Visiting Instructor
Stevens Institute of Technology	2005-2008	Graduate Assistant
TechnoProductions	2000-2003	President
LSI Logic	1998-2000	Senior Software Engineer
TechnoProductions	1996-1998	President
Ikos Systems Inc.	1994-1995	Senior Software Engineer
Giordano Automation	1992-1994	Systems Analyst
Clarkson University	1990-1991	Student Consultant
U.S. Navy	1988	Seaman

Publications

Patent Applications

- Michael de Mare. Iterative symmetric-key ciphers with keyed S-boxes using modular exponentiation. Patent application 12/051,626, 2008. USPTO Publication US-2008-0232597-A1.

Refereed Publications and Theses

- Michael de Mare. *Secure Set Membership Using 3SAT*. PhD thesis, Stevens Institute of Technology, December 2009.
- Michael de Mare and Rebecca Wright. Secure set membership using 3SAT. In *Eighth International Conference on Information and Communications Security (ICICS '06)*, pages 452-468. Springer, *Lecture Notes in Computer Science*, volume 4307, 2006.
- Michael de Mare. An analysis of certain cryptosystems and related mathematics. Master's thesis, State University of New York Institute of Technology, Dec. 2004.
- Josh Benaloh and Michael de Mare. One-way accumulators: A decentralized alternative to digital signatures. In *Advances in Cryptology – Eurocrypt '93* pages 274-285. Springer, *Lecture Notes in Computer Science* volume 765, 1993.

Technical Reports

- Josh Benaloh and Michael de Mare. Efficient broadcast timestamping. Technical Report. Clarkson University, 1992.

Honors

National Merit Scholar Letter of Commendation

Languages

C, C++, VHDL, Verilog, Perl, Scheme, L^AT_EX, OpenMP

Platforms

DOS, SunOS, Solaris, HP UX, Linux, NetBSD

Experience History

State University of New York Institute of Technology (2008-2009)

Course	Title	Terms Taught	Comment
CS108	Computing Fundamentals	Fall 08, Spring 09	C Programming
CS370	Software Engineering	Fall 08, Spring 09	
CS451	Distributed Computing	Spring 09	Distributed Models and Protocols
CS490	Information Assurance	Fall 08	Security and Cryptography

- Taught six courses over two semesters.
- Designed and developed curriculum for special topics class on information assurance including topics in computer security and cryptography. Developed this curriculum into a new class *CS381 Computer Security and Cryptography*.
- Designed and developed new curriculum for *CS451 Distributed Systems* to replace old, unused curriculum.
- Served on Grad Council.
- Supervised three senior capstone projects.

Stevens Institute of Technology (2005-2008)

- Filed thesis with library on December 15, 2009: *Secure Set Membership Using 3SAT*.
- Defended thesis on February 27, 2009: *Post-Quantum Cryptography Using Complexity*.
- Designed and developed many computational experiments in C++ and ran them on a Sun high-performance cluster.

- Successfully defended thesis proposal: *Post-Quantum Cryptography Using Complexity*.
- Attended training on writing software for Sun high-performance clusters.
- Invented Pineapple and Dragonfire block ciphers. Filed a full utility patent on the Dragonfire cipher. Implemented both ciphers in C++. The Dragonfire cipher has two novel techniques in cipher design.
- Designed and developed parallel differential cryptanalysis for a cluster in C++ and Common Lisp.
- Published *Secure Set Membership Using 3SAT* with Rebecca Wright at ICICS 2006. It appears in the proceedings published by Springer in *Lecture Notes in Computer Science* volume 4307 pages 452-468.
- Attended Canadian Quantum Summer School (Equips 2006).
- Research assistant May 2005-Summer 2008 studying post-quantum cryptography.
- Passed the PhD qualifying exams.
- Teaching assistant for CS434 Theory of Computation Spring 2005. Duties included grading, helping students, designing pages on WebCT, posting homeworks and quizzes on WebCT, assisting in the development of homeworks and quizzes, providing students with solutions to homework problems and quizzes and teaching lectures when the professor is out of town.
- Member Laboratory for Secure Systems.

TechnoProductions (2000-2003)

- Experimental programs to test experimental number theory algorithms.
- Perl scripts and CGI programs for comprehensive data management system.

LSI Logic (1998-2000)

- Assumed responsibilities of group leader when he was not available. These included managing engineers, reporting group status to management and conducting meetings.
- Maintenance of the connectivity API and the VHDL analyzer at LSI Logic
- Extensive support in the netlist database software including hierarchical editing capabilities for patching Engineering Change Orders from Avant! back into the original Verilog file. This is required because Avant! generates illegal Verilog names.
- Specified, designed and implemented a renaming system for Verilog names and a mapping system back to the original names to allow designs to be run through the Avant! place and route tools. This enhancement required changes to the Name Map API, and the connectivity database in the LSI front-end CAD toolset. This will be obsoleted when Avant! conforms to IEEE standards.

- Recognized by LSI Logic with an Engineering Excellence Award.
- Designed and developed a name map database and API for mapping names between four different hardware description languages with different lexical and syntax rules. This includes the capability to merge in additional name map files to allow IP core names to be mapped into the design. This database uses in-memory compression to allow large designs to fit within a 4G address space. The compression algorithm yields 3:10 compression on large (> 500MB) name map files.
- Enhancements to LSI's connectivity and network database including selected net extraction, outputting only one selected module and the modules it depends on, improved memory performance, and making ndl implicit signal naming deterministic.

TechnoProductions (1996-1998)

- Designed and developed a WAVES vector generator from digital simulation results for the IKOS Voyager digital simulator. This is part of an SBIR contract Ikos has with Wright Laboratories (USAF).
- Worked with Ikos and Cadence engineers to develop the Open Modeling Forum demonstration for the Design Automation Conference (DAC '96)
- Worked on fixing Software Problem Reports and providing new features on the Ikos Voyager VHDL simulator. VHDL simulators are used by electrical and computer engineers to simulate hardware designs at various stages before going to the foundry for production as an ASIC (Application Specific Integrated Circuit) or other form of hardware.
- Designed and developed a VSTIM simulation stimulus generator from VHDL simulation results in either standard mode or in the WAVES'96 (Waveform and Vector Exchange Standard IEEE 1029.1). This allows stimulus/response data to be captured from a VHDL or WAVES simulation and fed into the NSIM or SonSim products. This is part of an SBIR contract Ikos has with Wright Laboratories (USAF).

Ikos Systems Inc. (1994-1995)

- Designed Native Code Generation modules for a VHDL compiler. This compiler was developed by Ikos for its Voyager 3.0 and future products.
- Designed the VHDL Virtual Machine runtime environment for a VHDL compiler. This compiler was developed by Ikos for its Voyager 3.0 and future products.

Giordano Automation Corp. (1992-1994)

- Designed and developed fault symptom matrix generation utilities using designs produced by CAD which produce EDIF outputs.
- Designed and developed a utility for capturing structural information from VHDL gate level designs and producing diagnostics information from this.

- Designed and developed the C++ class library used for developing diagnostic utilities at Giordano Automation.
- Designed and developed an EDIF to VHDL translator in C++ for converting CAD/CAE information for use by WSTA. WSTA is the Navy's Weapons Systems Testability Analyzer which is used for analysis of the testability attributes of a design and the development of diagnostics for that design. Wrote the translator for the electronics on the Seawolf submarine, but it was used for many projects.
- Invited talk to Clarkson University on One Way Accumulators. One Way Accumulators are a class of cryptographic functions with applications including secure digital timestamping.
- Coauthored One Way Accumulators: A Decentralized Alternative to Digital Signatures with Josh Benaloh, who was a Professor at Clarkson University at the time. This paper was presented at Eurocrypt '93, and is available in the Eurocrypt '93 proceedings (Springer-Verlag Lecture Notes in Computer Science 765).