

Michael de Mare  
3365 Cortese Circle  
San Jose, CA 95127  
mikey@michaeldemare.com

## Educational Background

Ph.D. Computer Science Stevens Institute of Technology Jan. 2010 GPA 3.75

## Employment History

Employer	Period of Time	Title
Technoproductions	2009-present	President
Stevens Institute of Technology	2005-2008	Graduate Assistant

## 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<sup>A</sup>T<sub>E</sub>X, OpenMP

## Platforms

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

## Experience History

### 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*.
- Research assistant studying post-quantum cryptography and theory of computation Summer 2007.
- Research assistant studying symmetric key ciphers and quantum complexity Spring 2007.
- 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.
- Invented new method of constructing symmetric-key ciphers.
- 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.
- Research assistant studying post-quantum cryptography using NP-hardness Fall 2006.
- Attended Canadian Quantum Summer School (Equips 2006).
- Research assistant studying ciphers, elections and quantum computing Summer 2006.
- Research assistant studying impossibility of NP-complete ciphers Spring 2006.
- Research assistant studying secure secret ballot election schemes Fall 2005.

- Research assistant May 2005-Summer 2008 studying post-quantum cryptography.
- Passed the PhD qualifying exams.
- Research assistant studying the set membership problem, Summer 2005.
- 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.