

Vita

Michael de Mare

Michael de Mare was born in Brooklyn, New York on October 14, 1969. He has a Bachelor of Science from Clarkson University in Computer Science awarded May 1991, a Master of Science from State University of New York Institute of Technology in Computer Science awarded December 2004, and is a doctoral candidate at Stevens Institute of Technology in Computer Science. He is currently a Visiting Instructor of Computer Science at State University of New York Institute of Technology. He worked as a systems analyst at Giordano Automation from 1992 to 1994, as a senior software engineer at Ikos Systems from 1994 through 1995, for Technoproductions Inc. (consulting for Ikos Systems) from 1996 through 1998, and as a senior software engineer at LSI Logic from 1998 through 2000. His publications include *Efficient Broadcast Timestamping*, a technical report at Clarkson University, [1], *One-Way Accumulators: A Decentralized Approach to Digital Signatures* at Eurocrypt '93, [2] and *Secure Set Membership Using 3SAT* at the Eighth International Conference on Information and Communications Security (ICICS 2006), [5], as well as his masters thesis: *An Analysis of Certain Cryptosystems and Related Mathematics*, [3] and the patent application: *Iterative Symmetric-Key Ciphers With Keyed S-boxes Using Modular Exponentiation*, [4]. He was a National Merit Scholar Letter of Commendation winner and won an Engineering Excellence Award at LSI Logic.

References

- [1] Josh Benaloh and Michael de Mare. Efficient broadcast time-stamping. Technical Report TR-MCS-91-1, Clarkson University Department of Mathematics and Computer Science, 1991.
- [2] Josh Benaloh and Michael de Mare. One-way accumulators: A decentralized approach to digital signatures. In *Advances In Cryptology – Eurocrypt '93*, volume 765/1994 of *Lecture Notes in Computer Science*, pages 274–285. Springer, 1994.
- [3] Michael de Mare. An analysis of certain cryptosystems and related mathematics. Master's thesis, State University of New York Institute of Technology, Dec. 2004.
- [4] Michael de Mare. Iterative symmetric-key ciphers with keyed S-boxes using modular exponentiation. Patent application 12/051,626, 2008.
- [5] Michael de Mare and Rebecca N. Wright. Secure set membership using 3SAT. In *Proceedings of the Eighth International Conference in Information and Communications Security (ICICS 2006)*, volume 4307/2006 of *Lecture Notes in Computer Science*, pages 452–468. Springer, 2006.