

# The Quantum Fourier Transform and Factorization

John Watrous (jwatrous@cpsc.ucalgary.ca)

*University of Calgary*

*Department of Computer Science*

*Calgary, Alberta*

*T2N 1N4, Canada*

## **Abstract.**

Shor's algorithms for factoring integers and computing discrete logarithms are (thus far) the most significant achievements of the theory of quantum computation. In these talks I will discuss the principal component of these algorithms, the quantum Fourier transform, and describe how the quantum Fourier transform allows for efficient factorization of integers and computation of discrete logarithms. I will also briefly survey some of the other problems believed to be intractable for ordinary computers that can be efficiently solved with the help of the quantum Fourier transform.