SCIENCE SEMINAR

Thursday, January 24

Carson Taylor Hall room 322

will feature

Dr. Jean-Francois Biasse

Assistant Professor of Math - University of South Florida

Math Faculty Candidate

presenting

"Are Cryptosystems Based on Ideal Lattices Quantum-Safe?"

Shor's algorithm factors RSA integers and solves the Discrete Logarithm Problem (DLP) in quantum polynomial time. Therefore, alternatives to these cryptosystems must be developed to replace the current cryptographic schemes. One of the most interesting family of schemes that have been proposed for the replacement of RSA-based and DLP-based primitives relies on the hardness of finding short vectors in Euclidean lattices. This problem seems intractable, even for quantum computers, and it allows many interesting functionalities such as Fully Homomorphic Encryption. In this talk we report on recent results showing that finding short vectors can be significantly faster in certain ideal lattices when using a quantum computer.

Come at 3:30pm for refreshments, speaker at 4:00pm