Talk # 1

Wednesday, September 18, 2013

Prof. Jesse Berezovsky

How to break RSA encryption

RSA encryption is the "gold standard" cryptosystem, used for secure communication by everyone from internet users to banks to governments. In this talk, I will describe the RSA encryption scheme and how to break it. The strength of RSA encryption is based on the difficulty of finding the prime factorization of large numbers. This problem can be solved using a quantum computer. I will present the components needed to build a quantum computer, the elementary quantum gates used to "program" a quantum computer, and the factoring algorithm which permits efficient breaking of RSA encryption. Finally, I will discuss some efforts in my own lab towards making this type of quantum technology a reality.