**JEAN-FRANÇOIS BIASSE**, University of South Florida
*Quantum algorithms for number theory and their relevance to cryptography*

I will report on recent results about quantum algorithms for solving computational problems in number theory.

In a recent work in collaboration with Fang Song, I presented the first quantum polynomial time algorithm for computing the S-unit group of a number field for a given set of prime ideals S. This algorithm works for arbitrary classes of number fields, even with large degree. It implies polynomial time algorithms for computing the ideal class group, solving the so-called "Principal Ideal Problem" (PIP), computing ray class groups and solving some norm equations. I will discuss the relevance of the efficient PIP resolution method for cryptography.

In collaboration with David Jao and Anirudh Sankar, I also described a quantum algorithm which finds an isogeny between two given supersingular curves over a finite field. In some cases, this algorithm runs in subexponential time. This can be used to attack quantum-safe cryptographic schemes relying on the hardness of finding an isogeny between two given supersingular curves.