Speaker: Francesco Sica

Title: Factoring with (Less) Hints

Abstract: In recently published work I presented a new approach to integer factorisation, using knowledge of the factorisations of nearby integers.

In particular, I found that in order to factor $N=pq$, a product of two large primes, in time $O(N^{c+\epsilon})$ with $\epsilon>0$ arbitrarily small, it suffices to know the factorisations of the $O(N^{c+\epsilon})$ nearest integers to N. This is nontrivial as soon as $c<1/2$, and the published result is obtained with $c=1/3$. There are other variations of the same result where the factorisation of N is achieved faster at the cost of more hints, resulting in the fastest deterministic factoring algorithm, albeit conditional on those hints.

I will explain how this method works and how a recent idea will allow an improvement to a (yet to be computed but effective) $c<1/3$.

The methods used are analytic, in a departure from usual research in the area, and may signal an interesting paradigm in the study of integer factorisation.