Factoring numbers with periodic interferograms

Vincenzo Tamma
Univ. of Maryland, Baltimore County; Univ. degli Studi di Bari;
tammav1@umbc.edu

The security of codes, for example in credit card and government information, relies on the fact that the factorization of a large integer number N is a rather costly process on a classical digital computer. Such a security is endangered by the Shor's algorithm which employs entangled quantum systems to find, with a polynomial number of resources, the period of a function which is connected with the factors of N. We can surely expect a possible future realization of such a method for large numbers, but so far the period of Shor's function has been only computed for the number 15.

Inspired by Shor's idea, our work aims to methods of factorization based on the periodicity measurement of a given continuous periodic "factoring function" which is physically implementable using an analog computer.

In particular, we have focused on both the theoretical and the experimental analysis of Gauss sums with continuous arguments leading to a new factorization algorithm. The procedure allows, for the first time, to factor several numbers by measuring the periodicity of Gauss sums performing first-order "factoring" interference processes.

We experimentally implemented this idea by exploiting polychromatic optical interference in the visible range with a multi-path interferometer, and achieved the factorization of seven digit numbers (see figure). For each number N to factorize, the corresponding trial factors associated with the brightest wavelengths (maxima in the interferogram) are the factors.

The physical principle behind this "factoring" interference procedure can be potentially exploited also on entangled systems, as multi-photon entangled states, in order to achieve a polynomial scaling in the number of resources.