Plenary Lectures
Conférences plénières

DR. PETER SHOR, MIT
Quantum Money

Quantum money is a quantum cryptograph protocol with several players, one of whom we call the mint. We assume all participants have quantum computers. For a quantum money protocol, we need

1. The mint must be able to create a quantum money state (with an associated serial number)

2. A merchant holding the quantum money state and knowing the serial number must be able to verify that it is a valid quantum money state.

3. An aspiring counterfeiter having both the quantum money and the serial number cannot create two states which both pass the verification test.

Quantum money was first proposed in 2009. Since then, a number of quantum money schemes have been proposed, several of which have been broken. We will discuss the history of quantum money and sketch how some of the schemes work.

DR. GIGLIOLA STAFFILANI, Massachusetts Institute of Technology
A small window on wave turbulence theory

Wave turbulence theory is a vast subject and its goal is to formulate for us a global picture of wave interactions. Phenomena involving interactions of waves happen at different scales and in different media: from gravitational waves to the waves on the surface of the ocean, from our milk and coffee in the morning to infinitesimal particles that behave like wave packets in quantum physics. These phenomena are difficult to study in a rigorous mathematical manner, but maybe because of this challenge mathematicians have developed interdisciplinary approaches that are powerful and beautiful. I will describe some of these approaches and show for example how the need to understand certain multilinear and periodic interactions gave also the tools to prove a famous conjecture in number theory, or how classical tools in probability gave the right framework to still have viable theories behind certain deterministic counterexamples.