QSS52 - Eleni Diamanti - Questions & Answers

Eleni Diamanti

What is the practical advantage of a quantum internet over the classical internet?

ELENI: The quantum internet can be thought of as complementary to the classical internet. It is used for the exchange of information between quantum devices, for enhancing certain functionalities by offering for instance higher security guarantees, and for adding some new ones that cannot be achieved with only classical resources.

"Authentication" and "message encryption" that have to be combined with QKD can be only classical or they could be also quantum protocols?

ELENI: In practical scenarios considered today, both these functionalities are achieved with classical/post-quantum algorithms. For message encryption, the most common ones are one-time pad or AES symmetric encryption, and for authentication, post-quantum digital signatures. Some ideas for quantum-based authentication exist.

What is the main physical mechanism/reason for bounds in secret key rates?

ELENI: The secret key rate bounds for noisy (repeaterless) quantum channels are linked to fundamental capacity limits. I recommend these two papers that have established such bounds: https://www.nature.com/articles/ncomms15043, https://www.nature.com/articles/ncomms6235

Are there useful non-Gaussian states for CV-QKD?

ELENI: CV-QKD does not need non-Gaussian states. Protocols use coherent or squeezed states.

Are quantum repeaters in production? if not, when could mass production be expected?

ELENI: Quantum repeaters are still in Research&Development phase, there are no products yet and large-scale production cannot be expected for several more years. The main principles have been demonstrated over short (few meter) distances and significant efforts are deployed to improve their characteristics while also moving up the TRL scale.

What role does Space/satellites play for quantum communications and other quantum science?

ELENI: Satellites are of utmost importance in quantum communications as they open the way to global-scale networks by using them as (trusted or untrusted) nodes. Space-based communication is also important in quantum science for time and frequency transfer, Earth sensing and observation and tests of fundamental physics.

In photonic chips mentioned by you: do you have any nonlinear elements/crystals for generation of nonclassical light, entangled states?

ELENI: The photonic chips used for the CV-QKD system do not contain entangled-photon sources. They contain active elements like amplitude and phase modulators, and also passive elements like directional couplers, as well as on-chip Ge photodiodes for the coherent detectors.

Are there any reasons why do you use ALGaAs instead of LiNbO3, BBO nonlinear crystals?

ELENI: Entangled photon sources based on AlGaAs present a number of advantages, including broadband operation and generation of entangled states without off-chip operations. They were perfectly suited in the multiplexing-based entanglement distribution work presented in the talk thanks to their broad spectral band.

How many satellites could be needed to enable quantum internet?

ELENI: This depends on the orbit of the satellite used for the quantum network. A GEO satellite can cover the whole Earth but puts stringent constraints in terms of the loss budget. A few tens of LEO satellites would probably allow for a realistic solution in terms of geographic coverage and service availability (over day and night).

What is a minimum secret key rate that it is acceptable for commercial use?

ELENI: This really depends on the use case and the required security level, there is no single answer. Key rates achieved today by high-performance QKD systems are on the order of Mbit/s over metropolitan distances, which is sufficient for several applications but not for the encryption of high volumes of classical network traffic.

Quantum memory based repeater are the only option, can you have other kind of quantum repeaters?

ELENI: There are some works on all-optical quantum repeaters that rely on efficient single-photon sources rather than on matter-based quantum memories.

What is the necessary resource for quantum advantage in q. communication? entanglement? or it depends on the protocol

ELENI: This depends on the protocol. Among the protocols that I talked about and for which we have managed to demonstrate a quantum advantage, quantum coin flipping and quantum money can be performed without entanglement, and this is also the case for quantum communication complexity exploiting the coherent state mapping. Many other protocols, including anonymous transmission and other advanced functionalities, require entanglement.

What it is the importance of quantum communication networks in quantum computing?

ELENI: Quantum communication is necessary at small scale to connect smaller units within a large quantum processor, and at large scale for connecting quantum computers over long distances hence enabling for instance distributed quantum computing.

In your optical fiber experiment, this seems to use the dark fiber. Is it possible to use the usage of the existing optical fiber network?

ELENI: Yes, there are many works studying the coexistence of quantum and classical signals over the existing optical fiber infrastructure, with very promising results.

Can you also compensate for fluctuation in channels in satellite-to-ground QKD?

ELENI: Theoretically, the security analysis of QKD protocols can take fluctuations into account and study performance in their presence. Experimentally, adaptive optics techniques can be used for improving the coupling of light on the ground despite the wavefront distortion.