Applications of quantum networks
Alexey Gorshkov

By routing and processing photons, quantum networks (also called quantum internet) would allow for distributing quantum information and multipartite entanglement between multiple parties separated by potentially long distances. Here we list some applications of such networks.

**Secure long-distance communication.** Quantum networks, including linear quantum networks called quantum repeaters [1], will enable secure long-distance communication, with applications in commerce, national security, and counterintelligence.

**Anonymous communication of classical information (can do quantum, too).** This communication can be of two types. (1) Anonymous broadcast [2]: everyone receives the message but nobody (except of course for the sender) knows who sent the message and where the sender is. (2) Anonymous person-to-person communication [3, 4]: only the sender knows who sent the message and only the sender and the receiver know who received it.

**Secure communication with improved signal-to-noise ratio via quantum illumination** [5]. Alice prepares two entangled photons and sends one to Bob. Bob encodes a message onto the photon and sends it back to Alice. Alice can distinguish Bob’s photon from the noise more easily because she is holding its entangled twin.

**Superdense coding** [6]. In the presence of a shared entangled pair, we can communicate two bits of information by sending only one qubit. This reduces traffic by a factor of two (i.e doubles the information transferred).

**Distributed quantum computing** is carried out by quantumly linking many spatially distributed quantum computers. In some cases, quantum computers in general and distributed quantum computers in particular are believed to offer an exponential speed up over classical computers, with applications to solving numerous hard problems from drug design in biology, to materials design, to breaking cryptographic codes.

**Blind quantum computing** [7, 8], in which a client uses the computational power of a quantum computer in such a way that the computer learns nothing about the computation.

**Secure multiparty computation** [9, 10] allows a number of end users to solve jointly a problem, whose answer depends on the inputs of all the users, while keeping the inputs confidential. For example, suppose three business leaders have $A, $B, and $C, respectively, and want to decide whether they have enough money to buy together a company that costs $X, i.e. whether $A+B+C is larger than $X. However, they would like to answer this question without revealing to each other how much money each of them has. Secure multiparty computation over a quantum network allows the three business leaders to achieve this. Another example is voting.

**Quantum appointment scheduling** [11, 12]. Suppose two busy people are talking over the phone and trying to compare their calendars to schedule a joint meeting. They can find a mutually acceptable time much faster if they are communicating over the quantum internet.

**Quantum fingerprinting** [13]. Suppose two remote users want to verify whether they have two identical copies of some big piece of data, e.g. whether some records have been updated or tampered with. With quantum internet, this can be done exponentially faster than with classical communication by means of comparing exponentially small quantum fingerprints of the data instead of comparing entire data sets.

**Long-baseline interferometry in astronomy and other vision applications** [14]. A pair of optical telescopes works by physically bringing together and interfering photons arriving at the two telescopes. The angular resolution increases with the baseline, which is the distance between telescopes, but so does the loss experienced by photons that we are trying to interfere. Using quantum networks, or more specifically quantum repeaters [1], one can establish entanglement...
between the two telescopes and avoid these propagation losses by teleporting the photons from one telescope to the other for interference. This, in turn, allows one to increase the baseline and increase the resolution. More generally this entanglement-assisted long-baseline interferometry allows us to determine the position of a light source when the photons are scarce and propagation is lossy. In addition to applications in astronomy, this technique has applications in vision and reconnaissance from ground, air, or space to ground, air, or space.

Unforgeable quantum money [15]. The no-cloning theorem prevents cloning of quantum states. This allows banks to issue unforgeable quantum money in the form of quantum states, while quantum internet allows for the transmission of this money across the globe.

Distributed sensing and time-keeping. Quantum networks will also allow us to entangle remote clocks or sensors thus significantly improving their capabilities beyond those achievable with purely classical links. Such entangled clocks [16] or sensors may dramatically improve time transfer, navigation, search for oil/gas/minerals, and the monitoring of volcanos and earthquakes.

Bit commitment, remote coin flipping, and digital signatures. Quantum networks allow for bit-commitment with device-independent security [17]. A bit commitment scheme allows one to commit to a chosen value of the bit, but reveal that value only at a later time. Bit commitment allows two remote parties to participate in coin flipping: Alice commits to a call (heads or tails), but reveals what she committed to only after Bob tosses the coin. Bit commitment is also used in digital signature systems.

Quantum secret sharing of classical or quantum messages [18, 7] is a network cryptography protocol that splits a (classical or quantum) message between several parties so that only all parties together can read the message, while any subset of the parties cannot.

References


