

Quantum Teleportation Tutorial

By Travis S. Humble

Scientific advances supporting the growth of our nation's information infrastructure presently derive exclusively from features of classical physics. But in recent years, a new framework has emerged to develop information technologies that operate according to the more fundamental laws of quantum physics. The intersection of quantum physics with information theory has led to quantum information science, a revolutionary approach that provides insight into the "physics of information." More importantly, quantum information science provides opportunities to both enhance and radically alter our current capabilities for computation, communication, and sensing.

Quantum Information Science

Quantum information, like classical information, is built up from logical states, namely, 1's and 0's. These logical states represent information that is manipulated by an information processing device, e.g., a computer, where the bits of information are encoded into the physical system and controlled in an algorithmic manner. What distinguishes quantum information from classical information is how this encoding is accomplished. Current information processing devices rely on classical signals to encode the logical states, e.g., positive and negative voltages encode the 0's and 1's in classical computers. Such devices are well described by classical physics. Quantum information processing differs in that the physical systems used to encode bits of information behave according to the laws of quantum mechanics.

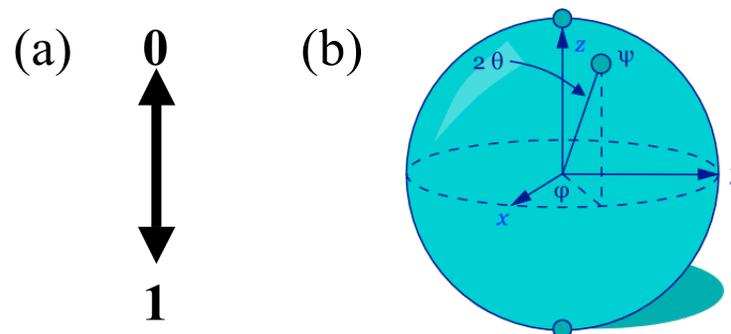


Fig. 1. Classical versus quantum bits. (a) In a classical setting, the logical states 0 and 1 are mutually exclusive and analogous to up and down positions. (b) In a quantum setting, the analog of the classical bit is the quantum bit, or qubit. The possible values of a qubit map onto the unit sphere, where the upper and lower poles of the sphere correspond to the logical states 0 and 1, respectively. The angles θ and φ define the orientation of the unit vector ψ .ⁱ

This distinction has dramatic consequences. Unlike classical bits, quantum bits, or *qubits*, can exist in superpositions of logical states. This feature implies that qubits need not encode a single value of either 1 or 0, but that they can simultaneously represent both logical states. In addition, quantum physics permits spatially separated qubits to behave synchronously even in the absence of physical contact. Albert Einstein famously referred to this feature as "spooky action at a distance," and Erwin Schrödinger first termed the underlying phenomenon *entanglement*. Entanglement has since become an important resource for speeding up algorithmic computations and streamlining communications.



Fig. 2. A hypothetical demonstration of entanglement, where Schrödinger's cat is subjected to nerve gas if the radioactive element in the lower panel emits a decay particle. Because the atomic decay process is quantum mechanical, the livelihood of the cat is indeterminate in the absence of observation. Both outcomes carry a non-zero probability that is simultaneously describable by the theoretical formalism of entanglement.ⁱⁱ

Quantum Information Technologies

The uniqueness of qubits and entanglement are fueling research and development into quantum information technologies. The foremost example of such technology is the quantum computer. A quantum computer uses superpositions of qubits to gain an exponential speed-up in computational performance as compared to classical computers. This is because a quantum computer is inherently parallel and computations are effectively performed on many different inputs simultaneously. Already a quantum algorithm has been discovered for enhancing the factorization of large numbers. This sole example has far reaching consequences for information security: Many variants of public-key encryption rely on openly sharing the product of two prime numbers since factorizing large numbers is considered exceedingly difficult to perform on a classical computer. If a quantum computer can surmount this computational challenge (and it appears that it can) then encryption techniques, like RSA and elliptic curve protocols, will one day be broken. Accordingly, the security of many communication networks will be compromised, as will the security of data previously encrypted using those techniques.

Quantum information technology is also breaking new ground in the field of communications. Quantum communication entails sending and receiving both qubits and classical bits using features unique to quantum information. One outstanding example is quantum key distribution. QKD uses the inherent randomness of quantum mechanics to construct a completely random string of classical bits. Acting like a one-time encryption pad, QKD generates strings of random bits that can be used to encrypt a classical message in a information-theoretically secure manner. It seems likely that QKD will replace the aforementioned computationally secured encryption techniques. But the extensive use of QKD for encryption may have drawbacks: whereas computational security can be overcome through sufficient computational capabilities, the perfect security of QKD precludes this prospect altogether. Thus, QKD could stymie intelligence gathering in situations that depend on the weakness of an encryption protocol.

Quantum Teleportation

A key technical capability fueling the advances afforded by quantum information science is quantum teleportation. Akin to its science-fiction namesake, quantum teleportation transfers objects between distantly separated locations. Unlike fictional accounts, however, quantum teleportation transfers information not matter. This point can be readily understood from an analogy with the fax machine: a fax machine transmits information on a piece of paper, not the paper itself. Similarly, quantum teleportation transmits information that is encoded into a quantum-physical system, not the system itself. These systems are most often single atoms and photons, though small molecular devices have been used as well. But what truly distinguishes quantum teleportation from conventional communication is that teleported data does not traverse the space between sender and receiver. Moreover, the teleported data is inherently encrypted in a perfectly secure way.¹ Naturally, these features make quantum teleportation of interest to the Intelligence Community. In particular, quantum teleportation underlies specific schemes for QKD and quantum computing.

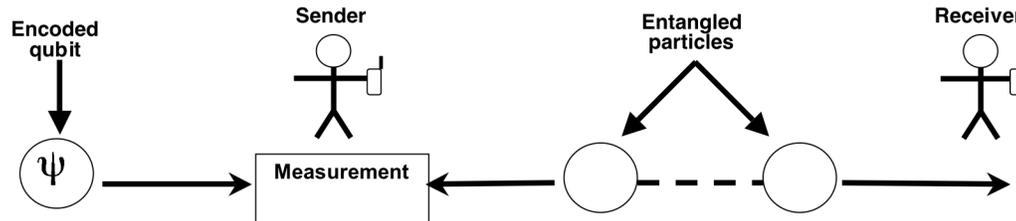


Fig. 3. A schematic of the quantum teleportation protocol using a qubit of information encoded into the left-most particle at the sender's station and a pair of entangled particles generated by an entanglement source located between sender and receiver. When one of the entangled particles interacts with the initial particle in a measurement device at the sender's station, the qubit of information is teleported to the third particle located at the receiver. The sender must convey two bits of classical information determined by the measurement outcome to the receiver so that the qubit can be decrypted. However, this classically communicated information does not betray the value of the teleported qubit.

Significant technical advances have been made since the first proposal for quantum teleportation in 1993. Foremost is the initial experimental demonstration of teleportation in 1997 using entangled photons to teleport data over a distance of 30 cm. Those tests, as well as other proof-of-principle experiments, have validated the principles underlying quantum teleportation and have led to even more elaborate application settings. As an example, teleportation using photons in free space was recently achieved over a distance of 144 km. As this distance approaches the altitude of low-earth orbit satellites (~300 km), quantum teleportation may one day enable satellites to be re-keyed using QKD techniques. Additional experiments have used quantum teleportation to transfer and store qubits of information in single atoms. These so-called quantum memory devices are fundamental components of quantum computer architectures and central to the concept of networked quantum communication channels.

¹ Because decrypting the teleported data requires a conventional communication channel, quantum teleportation cannot transmit information instantaneously and does not, therefore, violate the principles of general relativity.

Technical Description of the Research

Laboratory efforts have now matured to the point that the transition from proof-of-principle teleportation experiments to functioning full-scale quantum information devices necessitates realistic device designs that simultaneously satisfy the constraints imposed by size, cost, time, and application setting. In particular, the entanglement sources presently being used for testing quantum teleportation are highly inefficient and unsuitable for robust, real-world applications. Quantum teleportation using photons is perhaps the most advanced method to date, but practical implementations of this approach suffer from the available low-flux entanglement sources. Because entanglement is the vital resource for performing quantum teleportation, improvements to entanglement sources are paramount to the research and development of this technological capability.

The most prominent sources of entangled photons presently derive from the process of spontaneous parametric down-conversion. In SPDC, a high-energy pump photon supplied by an external laser interacts with a nonlinear optical crystal that induces the pump photon to decay into a pair of lower energy photons. With a properly designed source, the generated photons are prepared in a polarization-entangled state, i.e., the polarizations of the two photons are quantum-mechanically entangled. Additional restrictions are placed on the generated photons by conservation laws for energy and momentum, e.g., the energies of the down-converted photons must sum up to the energy of the initial pump photon.

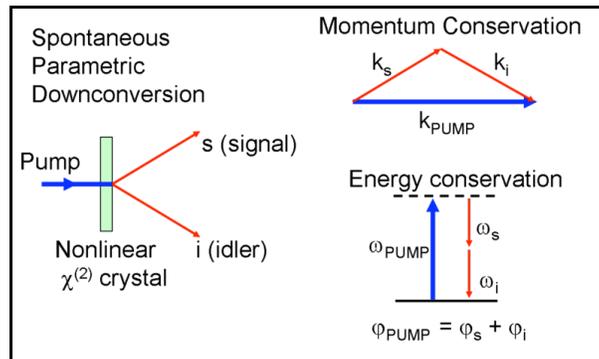


Fig. 4. The principles underlying spontaneous parametric down-conversion. A blue pump photon interacts with a nonlinear optical crystal that causes the production of two lower-energy red photons, termed the signal and idler. Conservation of energy and momentum restrict what photons are generated and lead to correlations in the properties of the down-converted photons.ⁱⁱⁱ

Though the conversion efficiency for SPDC is weak ($\sim 10^{-12}$ pairs/pump photon), pair production as large as 1 million pairs/sec can be achieved with modern techniques. However, the aforementioned restrictions on energy and momentum result in less-than-ideal characteristics for the photon pairs. Specifically, polarization entanglement is reduced when the frequencies and propagation directions of the two photons are clearly distinguishable. In laboratory experiments, such photon pairs are ultimately discarded by a filtering stage that selects only those few photons that are genuinely ideal. Notwithstanding the improvements that filtering garners for experimental results, the reduction in photon pairs impedes the efficacy of these entanglement sources. Therefore, an endeavor is underway to avoid filtering requirements by either (a) generating more ideal entangled photon pairs or (b) devising experimental techniques that are unaffected by the non-ideal photon pairs. The present theoretical research project envelopes path (b) and is being performed alongside an experiment-based project pursuing path (a).

The original proposal for quantum teleportation was a generalized prescription for using entanglement to transfer a qubit of information from a sender to a receiver. The proposal made use of abstract theoretical notation that could be easily extended to a wide variety of physical systems, and it intentionally avoided specifying the experimental details needed to achieve teleportation. In fact, it was not until several years later that all of the components necessary to implement teleportation with photons were realized experimentally. An apparent drawback to this timeline is that quantum teleportation was not explicitly intended for use with available photonic entanglement sources, which do not yet meet the stringent requirements imposed on the qubits in the initial proposal. In particular, presently available photons exhibit distinguishing information in the spectral and spatial degrees of freedom that are absent from the theoretical ideal.

The focus of the current research has been to reexamine the quantum teleportation protocol in the light of realistic entanglement sources. Working from the viewpoint that distinguishing information in the generated photons is often unavoidable, we have sought to optimize the use of current entanglement sources for quantum teleportation and related protocols. Our work builds from earlier discoveries that demonstrated how distinguishing information can be effectively erased through proper source design. Specifically, while distinguishing spectral information had been shown previously to reduce the measured entanglement of a single pair of photons (via Bell's inequality), a maximal measure of quantum interference is observed in certain situations (Hong-Ou-Mandel interference). Because quantum interference plays an important role in the teleportation protocol, it has been possible to extend those earlier considerations to this situation as well. Furthermore, we have found that interference effects in ostensibly related protocols (entanglement swapping, type-I fusion) are not similarly optimized, but are instead optimized by alternative source configurations.

While entanglement sources themselves will undoubtedly also improve, it seems unrealistic that said sources will ever be made free of the distinguishing information under consideration. Hence we anticipate that these results will influence the design of future high-fidelity, quantum-communication networks. Long-distance networks, in particular, are expected to make multiple calls to the quantum teleportation protocol. The accumulation of errors resulting from distinguishing information could be mitigated against by using the optimization procedures discussed here. In addition, the most prominent photonic approaches to quantum computation (circuit model and one-way model) each liberally utilize a variant of quantum teleportation, which can be similarly optimized by the approaches outlined here.

ⁱ The source for Fig. 1(b) is <http://en.wikipedia.org/wiki/Qubit>

ⁱⁱ The source for Fig. 2 is http://en.wikipedia.org/wiki/Schrödinger's_cat

ⁱⁱⁱ The source for Fig. 3 is http://en.wikipedia.org/wiki/Spontaneous_parametric_down_conversion