Entanglement and Quantum Key Distribution

By Justin Winkler

Entanglement in quantum mechanics refers to particles whose individual states cannot be written without reference to the state of other particles. Such states are said to be non-separable, and measurements of the state of one entangled particle alter the state of all entangled particles. This unusual phenomena has applications in quantum teleportation, superdense coding, and various other applications relating to quantum computing. Of some interest is how entanglement can be applied to the field of quantum cryptography, particularly quantum key distribution.

Quantum key distribution (QKD) is a technique that allows for secure distribution of keys to be used for encrypting and decrypting messages. The technique of QKD was proposed by Charles H. Bennett and Gilles Brassard in 1984, describing a protocol that would come to be known as BB84 [1]. BB84 was originally described using photon polarization states; no quantum entanglement was required.

BB84 requires measurement in two different orthogonal bases. Making use of the case of photon polarization, one basis is typically rectilinear, with vertical polarization at 0° and horizontally polarization at 90°, while the other basis is diagonal, with vertical polarization at 45° and horizontal polarization at 135°. Bit values can then be assigned as, for example, 0 for a vertically polarized photon and 1 for a horizontally polarized photon.

To distribute a key, the distributing party, Alice, creates a random bit in a random basis, sending a photon being 1 or 0 in either the rectilinear or diagonal basis. The photon created by Alice is received by Bob, who does not know the basis Alice used. Bob measures the photon's polarization, randomly choosing to measure in either of the two bases. Alice and Bob then discuss over a public channel which bases they chose to measure, and discard any bits where Bob did not measure using the same basis Alice used to create the photons.

This process allows for a secure channel for key distribution because anybody eavesdropping on the channel has to guess which basis to measure in. If Alice and Bob choose the same basis but the eavesdropper chooses a different basis then there is a 50-50 chance that Bob will measure a bit value different from what Alice sent. Thus, Alice and Bob have chance of detecting an eavesdropper by publicly comparing and discarding a certain number of bits for which they chose the same basis. This probability can bet set arbitrarily close to 1 by simply sending more bits. All bits remaining after discarding the publicly compared bits are used for the key.

A variant of quantum key distribution using entanglement was proposed by Artur Ekert in 1991 [2]. In this variant, entangled particles from some source are received by both Alice and Bob, who can measure polarization along different axes to achieve an effect similar to the BB84 protocol. In Ekert's original paper, Alice and Bob would measure polarization along three different angles. Alice would measure along 0°, 45°, and 90°, while Bob would measure along

45°, 90°, and 135°. Again, when Alice and Bob would publicly announce the angular orientations they used to measure along. Bits for the key would be the results of Alice and Bob's measurements when they used the same angular orientations. The results Alice and Bob obtained using different angular orientations could be publicly announced and used to construct the S value used in the Clauser-Horne-Shimony-Holt (CHSH) inequality [3]. By finding S, Alice and Bob could tell whether any eavesdropper had measured the polarization state as this would destroy entanglement and thus not allow violation the CHSH inequality. Various other QKD schemes based on entanglement were invented and shown to be secure against more refined attacks [4, 5], with an entanglement based QKD scheme being fully experimentally implemented and demonstrated in 2000 [5].

There are a wide variety of QKD approaches, but a common problem is the possibility of a photon number splitting attack. Because true single photon sources are currently impractical to implement in QKD experiments, such experiments typically make use of highly attenuated light so that the photon rate is low. Attenuating light in this way will not produce antibunched photons, so some photons will be produced in multiphoton bunches. In this case, it is possible for an eavesdropper to split off and store a single photon while the other photons are received by legitimate parties without any effect on their polarization [6]. The eavesdropper could then monitor the public announcement of bases and make measurements using the correct bases, leading to an undetected information leak. This sort of attack is referred to as a photon number splitting (PNS) attack.

With regards to a PNS attack, there are benefits to using an entanglement based QKD method. This is because the likelihood of simultaneously producing two entangled photon pairs is very low so that the effectiveness of a PNS attack is vastly reduced [5]. An additional benefit of entanglement schemes is they do not require a random number generator [5, 7].

The potential of entanglement based QKD schemes is well illustrated in an experiment conducted recently where QKD was achieved at a distance of 144 km in free space using entangled photons [7]. Polarization entangled photons were produced using a type II beta barium borate crystal with a Nd:vanadate laser. Photons were sent and received between two Canary Islands using telescopes aligned with tracking lasers. Researchers were able to demonstrate violation of the CHSH inequality and perform a secure key distribution.

It is clear that entanglement based quantum key distribution has great potential for practical implementation. Additionally, using entanglement reduces security concerns arising in single photon based key distribution schemes. Thus, the application of quantum entanglement to quantum key distribution is a topic of great relevance in modern quantum cryptography research.

-

Bibliography

[1] C. H. Bennett and G. Brassard, “Quantum Cryptography: Public key distribution and coin tossing”, in Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, p. 175 (1984)

[2] A. Ekert, Phys. Rev. Lett. 67, 661 (1991)

[3] J. F. Clauser, M.A. Horne, A. Shimony and R. A. Holt, *Proposed experiment to test local hidden-variable theories*, Phys. Rev. Lett. **23**, 880-884 (1969).

[4] Bennett, C. H., Brassard, G. & Mermin, N. D. Quantum cryptography without Bell’s theorem. *Phys. Rev. Lett.* 68, 557–559 (1992)

[5] Jennewein, T. *et al*. Quantum cryptography with entangled photons. *Phys. Rev. Lett.* 84, 4729–4732 (2000).

[6] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders. "Limitations on practical quantum cryptography." Physical Review Letters, 85(6):1330+ (2000)

[7] R. Ursin, et al. Nature Physics 3, 481 - 486 (2007)