Is optical quantum cryptography the ‘Holy Grail’ of secure communication?

Stamatios Kartalopoulos

Despite the belief of some researchers, issues exist that mean quantum-optical cryptography may not meet all the demands of secure communication.

Cryptography is a way to transform data to make it unintelligible to unauthorized recipients. The transformation is accomplished using a secret code, or key. Only authorized recipients with the same key can convert the text back to its original form so it can be read.

Before the digital era, there were various ways to transform alphanumeric text. For example, a simple key that says A=B, B=C, etc., transforms:

“THIS IS THE HIGHEST MOUNTAIN”
to:

“UIJT JT UIFIKHUF NPVOUBKO”

Digital data can be transformed with a digital key of equal length using an exclusive-OR (XOR) logic operation. Transforming:

10001101-10001010-11011010-10011110

with the digital key:

00110110-00100110-11110101-01100001

produces the encrypted string:

10111011-10101100-11101111-11111111

At the receiver, the same key is XORed with the encrypted string to produce the original text (try it!).

Secure communication can be established if the sender (Alice) and the rightful recipient (Bob) use the same key. The problem is that Bob must have the key before the encrypted message can be understood, but it’s often difficult to get that key to Bob securely. If the transmission channel is compromised by an eavesdropper (Evan), who gets hold of the key, he can decrypt the message. So finding secure approaches to key distribution (KD) is a vital part of cryptography.

In optical communications, modulated laser light is transmitted through fiber that acts like a conduit. One way to represent data is to use propagating photons in the fiber to represent a logic 1, and their absence a logic 0. A snapshot of the photons propagating in the fiber might show:

OOO O O OO O O O O O O O O

where O represents photons, and _ their absence. Although this technique can carry large amounts of data over long distances, it is not perfect. The photons can interact with local electromagnetic fields of the dielectric medium of the fiber, causing a variety of effects.1

Figure 1. The process that establishes a quantum key for Alice and Bob and its distribution using polarized photons. The shaded area shows what might happen if the fiber is compromised by Evan, and the false key.

Continued on next page
Quantum cryptography

According to the quantum-mechanical model of the atom, photons are produced when electrons transit from a higher to a lower energy state. This model also describes the principle of superposition of states, which says that between two extreme states (that we might think of as 1 and 0) there are a number of other quantized resonant states.

Optical communications can take advantage of the quantum-mechanical properties of photons, such as their polarization states or the entangled states of two photons that are propagating together. These states can play a key role in quantum cryptography (QC) and quantum key distribution (QKD).

Rather than simply using the presence and absence of photons to represent binary 1s and 0s, QC can use two or more polarization states—$P_1$, $P_2$, and so on—to represent a binary 1. Two or more other states, $-P_3$, $P_4$ and so on, represent a binary 0. Using multiple states to represent each symbol is more confusing for the potential eavesdropper. The data represented in the intermittent string of photons we took a snapshot of earlier would now be represented by a continuous stream of photons, whose polarization is as follows:


Using the quantum state of photons to represent binary data can help build cryptographic systems that have elegant ways of distributing keys securely and making it obvious when they have been compromised. In one scheme, shown in Figure 1, Alice sends Bob a test message in the form of a stream of photons that have been randomly polarized by a filter. Bob passes this stream of photons through his own randomly polarized filter and tells Alice the polarizations of the photons that emerge. Alice then tests her original message with Bob’s sequence, to deduce where there is match between the polarisation states of the two. She then tells Bob where in his bit sequence the polarizations match. Alice and Bob have now generated a secret that they share, but that was never shared directly over an open communications channel. This secret is used as the key to encode and decode their private communications, as in Figure 1.

Quantum theory says that it is impossible to observe something without altering its state. So if Alice sends a string of single polarized photons, Evan cannot measure their state, in order to copy them, without destroying it. Many believe that QC’s ability to share a secret key over a public channel without disclosing it (the distribution problem) and to make eavesdropping detectable make the approach the quantum the Holy Grail of cryptography. But does it work in real fiber-optic networks?

To answer this, we examined how the properties of propagating photons are affected in practical single-mode fiber networks. The fiber, although able to transport huge bandwidths over long distances, has its own deficiencies because of dopants, non-linearity and other photon/matter interactions. These may be exacerbated by pressure and temperature or by the actions of Evan, our eavesdropper, as in Figure 1. In typical multiwavelength transmisions the photonic signal power is attenuated due to scattering and absorption in the fiber. This is not the only problem: the polarization of photons cannot be sustained over long distances; due to fiber birefringence, photons traverse other optical and photonic components, which can alter polarization, phase, and entanglement; and photon entanglement or phase may be disturbed by optical amplifiers and other active components. Finally, multiwavelength transmission causes both linear and non-linear effects that affect photon properties and propagation.

Conclusion and future work

Although QC and QKD have great potential for cryptography, they also appear to have vulnerabilities in practical fiber-optic networks. These can be exploited to either eavesdrop on, or disable, the vital key distribution step. Developing a thorough understanding of these vulnerabilities may enable us to create countermeasures that could lead us to the ‘Holy Grail’ of cryptography, a truly robust and unbreakable cryptographic method.

Author Information

Stamatios Kartalopoulos  
ECE/TCOM  
The University of Oklahoma  
Tulsa, OK

Stamatios V. Kartalopoulos is currently the Williams Professor in Telecommunications Networking at the TCOM graduate program of the University of Oklahoma. Formerly, for 22 years, he was with Bell Laboratories. He holds 18 patents, has authored seven books, and written more than 90 papers. In addition he is an SPIE member, author, and speaker.

References