Published on *The National Law Review* https://natlawreview.com

China's Quantum Cryptography: Tales from (Quantum) Crypt

Article By:

Adam Waks

The dream of hack-proof communication just got a little closer to reality. On August 16, 2016, ***China*** launched the world's first "*quantum satellite*," a project the Chinese government hopes will enable it to build a communication system incapable of being hacked. Such a system, if perfected, would allow for encrypted communications between any two devices with absolute certainty that the encryption could not be broken, and with a built-in mechanism for alerting the sender/receiver if someone tried.If you are interested in truly understanding the mechanics of quantum cryptography, I would highly recommend the article "How Quantum Cryptography Works." For the purpose of this post, a very basic explanation is as follows:

In order to encrypt a two way communication, the sending party (who we will call "Alice") typically encodes a message using a key and sends the message to the receiving party (who we will call "Bob"), who then decrypts the message using the same key. Since modern technology makes it possible to engineer almost unbreakable keys, the best way for an eavesdropper (who we will call "Eve") to access the message is to find the key itself, which is vulnerable because it also needs to be communicated between Alice and Bob, but can't itself be encrypted, or else Bob won't be able to use it.

Quantum cryptography would allow Bob and Alice to use a new key for every message AND guarantee that if Eve tries to intercept the key, they will know. Quantum entanglement is a physical phenomenon that can cause certain particles to become "entangled" such that a change in one will elicit a predictable change in the other, no matter how far apart the entangled particles are, and without any measurable (by current scientific standards) communication between them. If Alice and Bob share entangled particles, Alice can transmit the information for a new key to Bob for every communication by altering the directional spin of her particles, which in turn will alter the spin of Bob's particles. A complicated process of measuring particle spin and cross-checking information between Alice and Bob (more fully explained in the article linked to above) is then used to generate the key.

Since so far as science is currently aware there is nothing "communicated" between the entangled particles, there is nothing for Eve to intercept unless she can actually access Bob's particles. Meanwhile, Heisenberg's uncertainty principle states that anytime the spin of one of these particles is measured, the very act of measuring it changes the spin of that particle. This means that if Eve does manage to physically access Bob's entangled particles and measures them to try and get Alice's key before passing the particles back to Bob, Bob will know the particles were intercepted because

the key he thinks he got from Alice won't work to unlock Alice's message after he and Alice cross-check their information, since Eve's measuring of Bob's particles caused the spin of those particles to change. Furthermore, since Eve is not able to cross-check her information with Alice, even if she is able to listen to Bob and Alice cross-checking their information, Eve will not be able to use her information to formulate the correct key to decode Alice's message.

The ability to send completely secure messages between any two points has myriad applications for data security. From a commercial standpoint, it could mean the ability for enterprises to remote access data without fear of interception. It could also mean an increase in the security of customer information (especially information that is legally required to be protected, such as personally identifiable information) and a corresponding decrease in the risk of a security breach that might result in damage to a company's brand, increased compliance costs, or potential litigation awards and expenses. For consumers, it could mean the ability to communicate private information securely in an age where so many online transactions require the sending of sensitive information over the internet.

More troubling (or liberating, depending on your point of view) are the challenges quantum cryptography poses for law enforcement and national security. Agencies such as the CIA, FBI, and NSA currently depend on access to third party data networks, such as e-mail clients and telecommunication companies, for a large part of their data collection and monitoring activities. Under the "third-party doctrine" when Alice sends a message to Bob, if a copy of that message is kept by the medium they use to communicate (e.g. by Alice's e-mail client), a government agency can request a copy of that information directly from Alice's e-mail client without needing to get a warrant, and without telling Alice or Bob about the request. Quantum cryptography could allow Alice to send an encrypted message to Bob such that, even if a government agency gets a copy of the message itself from Alice's e-mail client, they will not be able to decrypt it without help from either Alice or Bob.

Quantum cryptography still has a long way to go before it lives up to its promise, and there will almost certainly be bumps along the way. Yet, if the Chinese satellite launch does kick start the quantum cryptography revolution, commercial enterprises, consumers, governments, hackers, and lawyers alike will need to find ways to respond to the new challenges it creates.

National Law Review, Volume VI, Number 243