Joel George

004786402

Cost Effective Quantum Moves a Step Closer: Report

The subject of this report was an article published by IOP Publishing entitled, Cost Effective Quantum Moves a Step Closer. This article focused on a paper written by a team of Canadian and American researchers who have proven Measurement Device Independent Quantum Key Distribution (MDI-QKD) to be both a system that works practically with materials that are accessible to most laboratories. To understand MDI-QKD, though, a solid foundation in quantum mechanics must first be established. In classical computing, the type of computing that is used in almost every commercially available computer, the smallest unit of data is called a bit, and a bit can hold either a 0 or 1. In quantum computing, the smallest unit of data is called a qubit. A qubit is just any quantum system that can exist in two states: for example, a photon that is polarized vertically or horizontally. The interesting aspect of qubits is that because they are quantum systems, they have the property of superposition, which essentially states that until measured, a quantum system does not exist as either one state or another, but in a probabilistic mesh of the two. In other words, instead of being either a 0 or a 1, qubits exist as with a 30% chance of the qubit being a 0 when measured and a 70% chance of it being a 1 when measured (these percentages were assigned arbitrarily, they could be any percentages that add up to 100%). The ramifications of this technology are more understandable when comparing 3 bits to 3 qubits. Both 3-unit systems have 8 possible different configurations of 1s and 0s. The 3-bit system can only hold 1 of those 8 different configurations, while the qubits can hold all those configurations *at the same time*, because of superposition.

Superposition is one big aspect of quantum computing that makes it an incredible step up from classical computing. However, this major advancement in technology poses a threat to current methods of security, because many classical cryptography systems rely on computational limitations that quantum machines may be able to bypass. For example, RSA encryption relies on the fact that it is inordinately time consuming to factorize large prime numbers. Shor's algorithm, a prime-number factoring algorithm specifically designed for quantum computers, can factor a large prime number in time n^3, where n is the number of bits in the large prime number, while classical computers take an exponential amount of time to factor an n-bit prime number. In other words, quantum computers have the potential to crack RSA encryption, amongst other classical cryptography methods.

In order to stay one step ahead of hackers, quantum scientists developed the theoretically unbreakable cryptography system called Quantum Key Distribution (QKD). This method of key distribution addresses the current weak point that quantum computing has opened in current information sharing networks. With current information sharing networks, if Charlie wants to send a message to Bob, Charlie would first encrypt the message using a symmetric key, encrypt the key using RSA encryption, and then send the encrypted key and the encoded message to Bob across publicly accessible communication lines. Bob would then decrypt the symmetric key and then the message on his side of the network. Because quantum computers have the potential to decrypt the symmetric key that is sent across publicly accessible lines, QKD addresses this issue.

QKD is best explained by example. Imagine Alice wants to send Bob a message. First, she must send him the key that she will use to encode the message. To create this key, Alice generates randomly polarized photons. Each polarization corresponds to a certain encoded value. Alice records the filters use to polarize the photons, and then sends them across to Bob. Bob is now receiving a string of photons. To correctly decode the value encoded onto a photon, Bob must feed the photon into the detector specifically

created for that polarization. For example, if a photon is polarized horizontally and encodes a 1, to correctly decode this 1, Bob must feed the polarized photon into a detector built for horizontally polarized photons. If Bob accidentally feeds the photon into a detector built for vertically polarized photons, the detector will output either 0 or 1; there is an equal probability of either output, because the detector cannot correctly process the photon.

The problem arises with current technological capabilities – it is not possible for Bob to determine the polarization of the photons. Therefore, he must simply guess the polarization of each photon he receives and thus feeds the photons at random into the detectors that he has. Now, Alice has her string of photons, which encode a certain key, and Bob has his string. Only approximately 50% of the values in Bob's string will correspond with Alice's, so to coordinate strings with Alice, Bob sends Alice the order of detectors that he used when decoding her photons. Alice will then compare that list with the order of filters that she used, and will tell Bob when they deviated in terms of detector-filter polarizations. The two will then remove the values that were generated by different detector-filter polarizations; the remaining values should be synchronized across the two of them and will be their secret key.

This system is theoretically unbreakable for two main reasons. Firstly, the actual key values are never communicated across the network. Bob and Alice only share the order of filters and detectors that were used, so without the randomly polarized photons, any attacker that taps into the network and gains this information will not be able to do anything productive with this. Secondly, if an attacker does tap into the quantum channel and starts reading the randomly polarized photons, the laws of physics ensure that this attack will be detected. Qubits have the interesting property that when they are read, the value encoded on them is destroyed. Therefore, if the attacker was to read the photons that were going to Bob, Bob would realize this, as the photons he was receiving would have no encoded values on them. To maintain the illusion that the system is not under attack, the attacker may generate randomly polarized photons of their own and send them to Bob. However, since the attacker does not know the original polarization of the photons they received, they must randomly polarize photons of their own. Because the photon strings that are shared are lengthy, it is guaranteed that the attacker will polarize a photon incorrectly; the polarization of the photon that the attacker generates will not match the original polarization that Alice sent. When Bob is decoding this lengthy string of photons that was sent to him from the attacker, there will be times when he feeds the photon into the detector that would've been correct if he was receiving Alice's original string of photons, but registers incorrectly because he is receiving the incorrect string of photons generated by the attacker. As part of the BB-84 Protocol, Bob and Alice will share a subsection of the strings that they generated with each other. Alice and Bob will notice values where Alice and Bob did in fact use the correct filter-detector sequence, but they still got different values. This kind of deviation indicates that an attacker did in fact hit the system, and Alice and Bob will be alerted to that without sharing any sensitive information across the network.

While theoretically QKD is unbreakable, the physical implementations of this system is highly susceptible to hacking. Side channels, which are hacks that exploit physical weaknesses in the system, are QKD's biggest weakness. There is a side channel called the "blinding attack", which works by directing a laser into Bob's detectors. Without going into too much detail, this attack allows the attacker to tap into the quantum channel undetected. To fix this, MDI-QKD was proposed. Essentially, MDI-QKD relies on a central, untrusted node that is remote to both Alice and Bob, instead of local detectors that are prone to being exploited. The upgrade is based upon a similar foundational principle of QKD. If the untrusted node chooses to interfere with the processing of Alice and Bob's information, the inconsistencies generated by the attacker will be detectable. This is an improvement to QKD because the processing of the photons no longer relies on detectors that are prone to blinding attacks, but rather relies on technology in a removed

node, so that if that node is tampered with, the tampering will be detected in Alice's and Bob's secured laboratories. Because the detection systems are removed instead of built in to Alice's and Bob's sites, they can remotely monitor whether an attack occurred, without getting hit by the attack themselves.

The focus of the report was on MDI-QKD, and essentially discussed the researcher's success in implementing it with equipment that is available to a general scientific audience. This is a major breakthrough in making quantum computing, and the equally important field of quantum cryptography, more accessible reality. While protecting data is important on national scales, this kind of research is pertinent to the layperson too. All of the credit card and personal information that exists about any modern Internet user is protected by classical systems of cryptography, which may be susceptible to quantum computers in the future. By pushing the progress of quantum cryptography, this data can be 'future-proofed'. Instead of relying on computational limitations of computers, as classical cryptography systems do, quantum cryptography relies on the fundamental laws of physics to protect and encode. This, to me, is an amazing utilization of the world around us, and is an ingenious step towards pushing the progress of computer science even further on.

Works Cited:

1. Valivarthi, Raju, et al. “A Cost-Effective Measurement-Device-Independent Quantum Key Distribution System for Quantum Networks.” Quantum Science and Technology, vol. 2, no. 4, 2017, doi:10.1088/2058-9565/aa8790.
2. Merali, Zeeya. “Hackers Blind Quantum Cryptographers.” Nature, 2010, doi:10.1038/news.2010.436.
3. Lo, Hoi-Kwong, et al. “Measurement-Device-Independent Quantum Key Distribution.” Physical Review Letters, American Physical Society, 30 Mar. 2012, doi.org/10.1103/PhysRevLett.108.130503.
4. Diamanti, Eleni, et al. “Practical Challenges in Quantum Key Distribution.” Npj Quantum Information, vol. 2, no. 1, 2016, doi:10.1038/npjqi.2016.25.