Is quantum mechanics a friend of the Internet?

Fumiya Hanamura

Nowadays, our lives totally depend on the Internet. One of the inevitable problems when we use the Internet is the problem of security, because all the information we send through the Internet is just carried through the air or cables, as electromagnetic waves, without any physical protection, therefore in principle accessible for everyone. Hence, we need some encryption of the information to securely communicate across the Internet. Currently, the Internet security is mainly based on the method called RSA cryptography, named after the three information theorists who invented the method. However, the security of RSA cryptography is not rigorously proven, because it just relies on the hardness of finding the prime factorization of large numbers with current computers and algorithms. Therefore, we cannot deny the possibility that someday, someone will find a clever algorithm to solve the prime factorization and break the RSA encryption, revealing all the secret information carried through the Internet, including your personal e-mail message, and your net banking password. In that sense, our prosperous IT society is built on thin ice. Worse still, it has been proven that it is impossible to make information theoretically secure, i.e., fundamentally unbreakable, cryptography within the current communication system based on classical electromagnetism.

Quantum mechanics is the key to this problem, as it can be both an enemy and a savior. Quantum mechanics is a fundamental theory of physics, which describes the strange behavior of microscopic systems at the scale of atoms, and our intuitions sometimes do not apply there. It has been shown that using quantum mechanics, one can make computers –called quantum computers— which can efficiently solve some problems which cannot be efficiently solved by current computers. Quantum computers are considered to offer many useful applications including drug discovery, artificial intelligence, and traffic optimization, and certainly will play a leading role in the next-generation information technology. The problem is, quantum computers can also efficiently solve the prime factorization problem, which means that one can break the RSA encryption using quantum computers. Fortunately, the current state-of-the-art quantum computer can only solve prime factorization of numbers as large as at most 21

(=3×7, trivial!) [1], and far from solving currently used RSA cryptography, which requires the prime factorization of numbers with more than 200 digits. However, quantum computers are actively researched, and their performance is advancing day by day, and someday may break the RSA cryptography used on the Internet.

On the other hand, quantum mechanics also provides us a workaround for the problem. In quantum mechanics, one cannot make an observation on a quantum state without changing the state. Using this property, one can consider encrypting information into a quantum state and send it as a message. If someone attempts to eavesdrop on this message, it can be always detected, because the state after eavesdropping changes. This method is called quantum cryptography and has been rigorously proven to be secure (even if the eavesdropper uses a quantum computer!) as long as quantum mechanics is correct, which is clearly far more plausible than the hardness of the prime factorization. Someday, all the RSA cryptography used on the Internet may be replaced by quantum cryptography, ensuring the absolute security of the Internet.

One may wonder, the day quantum computers break the RSA cryptography, or the day quantum cryptography completely replaces the RSA cryptography, which comes earlier? Of course, this is an essential question. Fortunately, it seems that the latter comes earlier, as it is much easier to implement quantum cryptography rather than building a large-scale quantum computer which can be used for performing prime factorization of large numbers. Indeed, there are already some experimental achievements of quantum cryptography. For example, one of the most promising implementations of quantum cryptography is the one using light, because light has strong quantum nature, and can be efficiently transmitted over a long distance. In 2015, B. Korzh et al. conducted an experiment to transmit quantum-encrypted messages through optical fiber over a distance of more than 100 km, and they achieved 12 kbps rate of transmission [2]. In 2017, S. Liao et al. sent quantum-encrypted messages from a satellite to the Earth over a distance of 1200 km [3]. Although the transmission rate is still slow compared to our daily classical communication, there is no doubt that quantum cryptography will be put into practice in the near future.

Therefore, it is sure that there must come a day when we can safely transfer our important secret information across the Internet using quantum cryptography, without fear of a genius hacker doing prime factorization at high speed, or a mad scientist who

has secretly invented the quantum computer. Until then, it is important to keep in mind that the Internet security on which we are hugely relying in our daily lives is not an absolute one.

Source: https://www.irasutoya.com

[1] Amico, Mirko, Zain H. Saleem, and Muir Kumph. "An Experimental Study of Shor's Factoring Algorithm on IBM Q." *arXiv preprint arXiv:1903.00768* (2019).

[2] Korzh, Boris, et al. "Provably secure and practical quantum key distribution over 307 km of optical fibre." *Nature Photonics* 9.3 (2015): 163-168.

[3] Liao, Sheng-Kai, et al. "Satellite-to-ground quantum key distribution." *Nature* 549.7670 (2017): 43-47.