Post-Quantum Cryptography: Development and Use of Encoding Protocols

Guerra, Henrique (School: Colegio Dante Alighieri)

In the 1940s, Alan Turing became a big figure of World War II, but it didn't happen in the battlefield: by cracking Nazi's codes, he provided England an enormous strategic advantage, cementing the courses of the war. Since then, the cryptography which decided wars gained even more importance: due to Turing's big invention, the computer, and to the internet, information's transmission got stratospheric scales, as well as the codes that protect it. Currently, the most used cryptography protocol is RSA, which safety underlies on the fact that big numbers' factoring, specially semiprimes, is extremely hard for classic algorithms. However, quantum technologies development would make the use of Shor Algorithm - which uses quantum properties to do the task way faster than what's possible today - viable, compromising online data's safety. There already exist quantum resistant protocols which are extremely safe and able to overcome this obstacle; nonetheless, its implementation will take time and require an infrastructure that doesn't exist yet, so that this will only happen in a distant future. Shor Algorithm, on the other hand, doesn't depend on global infrastructure, but only on a few cutting-edge quantum computers, in a way that it will probably threat data's safety in mid-term, way before post-quantum cryptography implementation. Therefore, this work's intent is to improve Shor-resistant cryptographic methods that are already used commercially (in small scale), namely BB84 and E91, and to discuss ways to use them in present cities optic fiber networks, with little to no modifications. Keywords: Quantum Physics, Quantum Entanglement, Cryptography