Quantum computing is the next big leap

Traditional network infrastructures and cybersecurity standards will be compromised if quantum computing becomes viable, the reason why quantum R&D is a key factor of EU's digital strategy.

Our most sensitive information, say banking or browsing data, is kept secure by rather resilient encryption methods. With current computing capabilities, it is a very difficult task for a computer to run the necessary math in order to extract information from encrypted data. That is not the case, however, with quantum computing.

At their smallest, computers are made up of transistors, which process the smallest form of data: *bits* or 0s and 1s. Contrary to regular machines, which operate in *bits*, quantum computers process *qubits*, which carry not *one* of those two values, but *any* of those two. Because they operate in *qubits*, they are able to process data unseemingly faster.

If a regular computer were to guess the combination of two *bits*, it would take, at worst, four different tries (2^2 – 00, 01, 10, 11) before guessing it. A quantum computer would only require the square root of that, because each *qubit* carries *any* of the two values. When processing large numbers this makes a huge difference.

While it is not expected that quantum computers will be commercially viable or even sufficiently developed anytime soon to squander computing as it is today, a number of the encryption algorithms used today are not quantum-resistant.

Having considered the above, it is not uncalled for that organizations are rethinking their cybersecurity standards in order to protect their data in view of new developing technologies, namely quantum computing.

Portugal signed up for EU's Quantum Communication Infrastructure initiative ("**EuroQCI**"). The initiative trusts on developing a network over the next ten years for sensitive information to be shared. As with anything that may be ill-used, quantum computing poses a serious cyberthreat. EuroQCI will use quantum technologies to ensure the secure transfer and storage of sensitive information. As computer parts are now as small as the size of an atom and current computing is reaching its physical limits, the EuroQCI aims at making quantum computing and cryptography a part of conventional communication networks, which is in line with Portugal's strategy to strengthen the country's digital ecosystem.

Objective number one of Portugal's National Cybersecurity Strategy is to ensure national digital resilience by leveraging inclusion and cooperation in order to bolster the security of cyberspace in view of threats which may jeopardize or cause disruption of networks and information systems essential to society. Currently, the EU's *Study on the System Architecture of a Quantum Communication Infrastructure* (within the EuroQCI initiative) is open for contributions on the future of quantum network infrastructures. The consultation is open until 10 June 2020.

Contacts

João Macedo Vitorino
jvitorino@macedovitorino.com

Pedro Ramalho de Almeida
palmeida@macedovitorino.com

André Feiteiro
afeiteiro@macedovitorino.com