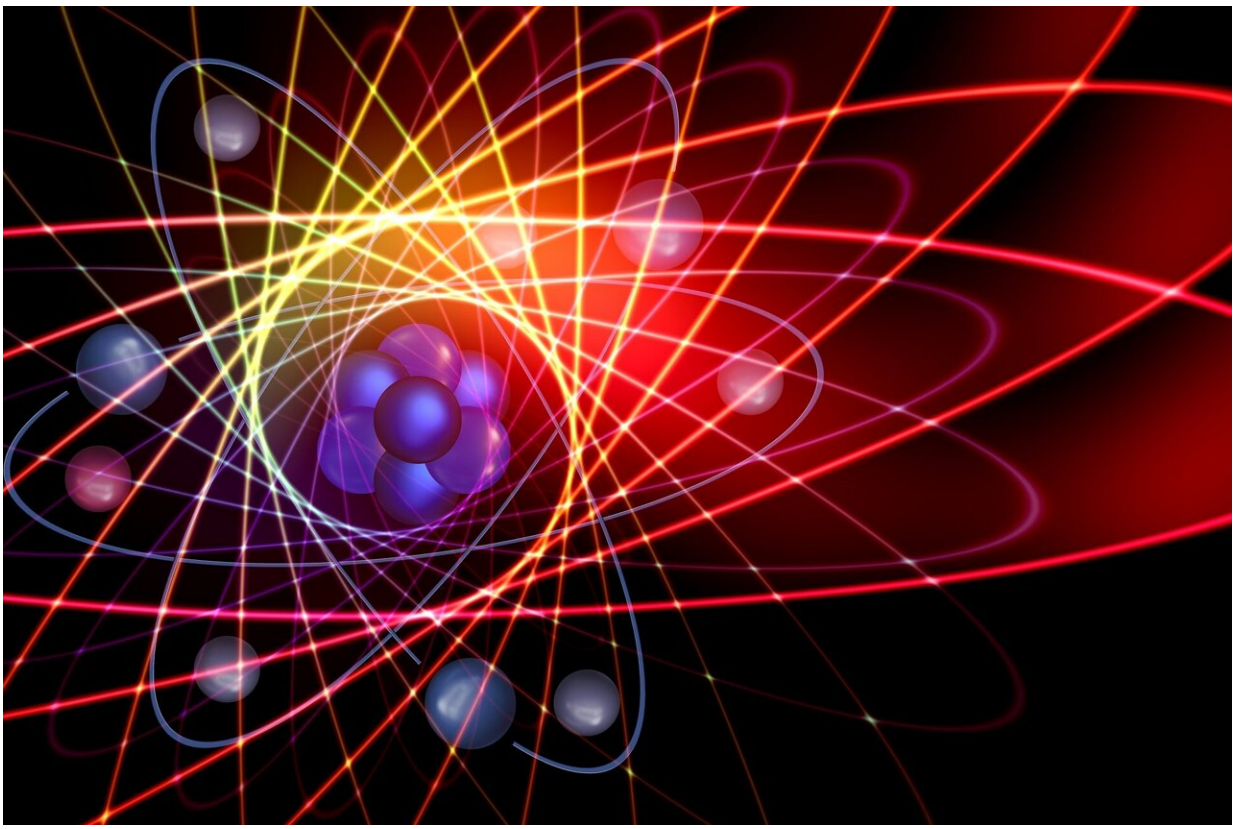
Quantum computers threaten our whole cybersecurity infrastructure: Here's how scientists can bulletproof it

January 12 2023, by Antonio Acín



Credit: Pixabay/CC0 Public Domain

Thirteen, 53 and 433. That's the size of *quantum computers* in terms of quantum bits, or qubits, which has significantly grown in the last years

due to important public and private investments and initiatives. Obviously, it is not only a mere question of quantity: the quality of the prepared qubits is as important as their number for a quantum computer to beat our existing classical computers, that is, to attain what's called the "quantum advantage". Yet it is conceivable that soon quantum-computing devices delivering such an advantage will be available. How would this affect our daily lives?

Making predictions is never easy, but it is agreed that *cryptography* will be altered by the advent of quantum computers. It is an almost trivial statement that privacy is a key issue in our information society: every day, immense amounts of confidential data are exchanged through the Internet. The security of these transactions is crucial and mostly depends on a single concept: complexity or, more precisely, computational complexity. Confidential information remains secret because any eavesdropper wanting to read it needs to solve an extremely complex mathematical problem.

In fact, the problems used for cryptography are so complex for our present algorithms and computers that the information exchange remains secure for any practical purposes—solving the problem and then hacking the protocol would take a ridiculous number of years. The most paradigmatic example of this approach is the RSA protocol (for its inventors Ron Rivest, Adi Shamir and Leonard Adleman), which today secures our information transmissions.

The security of the RSA protocol is based on the fact that we don't yet have any efficient algorithm to factorize large numbers—given a large number, the goal is to find two numbers whose product is equal to the initial number. For example, if the initial number is 6, the solution is 2 and 3, as 6=2x3. Cryptographic protocols are constructed in such a way that the enemy, to decrypt the message, needs to factorize a *very* large number (not 6!), which is at present impossible to do.

If computing devices are built for that would allow current cryptography methods to be easily cracked, our current privacy paradigm needs to be rethought. This will be the case for quantum computers (once an operational quantum computer exists, that is): they should be able to break RSA because there is a quantum algorithm for efficient factorisation. While classical computers may need the age of the universe to such a problem, *ideal* quantum computers should be able to do it in a few hours or maybe even minutes.

This is why cryptographers are developing solutions to replace RSA and attain *quantum-safe security*, that is, cryptographic protocols that are secure against an enemy who has access to a quantum computer. To do so, there exist two main approaches: *post-quantum cryptography* and *quantum key distribution*.

How to encrypt information in a world equipped with quantum computers

Post-quantum cryptography maintains the security paradigm based on complexity. One should look for mathematical problems that remain difficult for quantum computers and use them to construct cryptographic protocols, the idea again being that an enemy can hack them only after a ridiculously large amount of time. Researchers are working hard to develop algorithms for post-quantum cryptography. In fact, the National Institute of Standards and Technology (NIST) initiated a process to solicit and evaluate these algorithms and the chosen candidates were announced in July 2022.

Post-quantum cryptography presents a very strong advantage: it is based on software. It is therefore cheap and, more importantly, its integration with existing infrastructures is straightforward, as one only needs to replace the previous protocol, say RSA, by the new one.

But post-quantum cryptography also has a clear risk: our confidence on the "hardness" of the chosen algorithms against quantum computers is limited. Here it is important to recall that, strictly speaking, none of the cryptographic protocols based on complexity are proven to be secure. In other words, there is no proof that they cannot be solved efficiently on a classical or quantum computer.

This is the case for factoring: one can't rule out the discovery of an efficient algorithm for factorization that would enable a classic computer to break down RSA, no quantum computer required. While unlikely, such a possibility cannot be excluded. In the case of the new algorithms, the evidence of their complexity is much more limited, as they have not yet been intensively tested against smart researchers, much less quantum computers. Indeed, a quantum-safe algorithm proposed in the NIST initiative was later cracked in an hour on a standard PC.

Exploit the laws of quantum physics to secure communications

The second approach for quantum-safe security is *quantum key distribution*. Here, the security of the protocols is no longer based on complexity considerations, but on the laws of quantum physics. We therefore speak of quantum *physical security*.

Without entering into the details, a secret key is distributed using qubits and the protocol's security follows from the Heisenberg uncertainty principle, which implies that any intervention by the eavesdropper is detected because modifies the state of these qubits. The main advantage of quantum key distribution is that it is based on quantum phenomena that have been verified in many experimental labs.

The main problem for its adoption is that it requires new (quantum)

hardware. It is therefore expensive and its integration with existing infrastructures is not easy. Yet important initiatives are taking place for the deployment of quantum key distribution at a European scale.

Which approach to take? This question is often presented as an either-or choice and even in this article, you may have given this impression too. However, our vision is that the right way to go is to look for the combination of post-quantum and quantum key distribution. The latter has shown us that quantum physics provides us with new tools and recipes to truly safeguard our secrets. If the two approaches are combined, hackers will have a *much* more difficult time, as they will have to face both complex computational problems and quantum phenomena.

This article is republished from The Conversation under a Creative Commons license. Read the original article.

Provided by The Conversation

Citation: Quantum computers threaten our whole cybersecurity infrastructure: Here's how scientists can bulletproof it (2023, January 12) retrieved 18 April 2024 from https://phys.org/news/2023-01-quantum-threaten-cybersecurity-infrastructure-scientists.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.