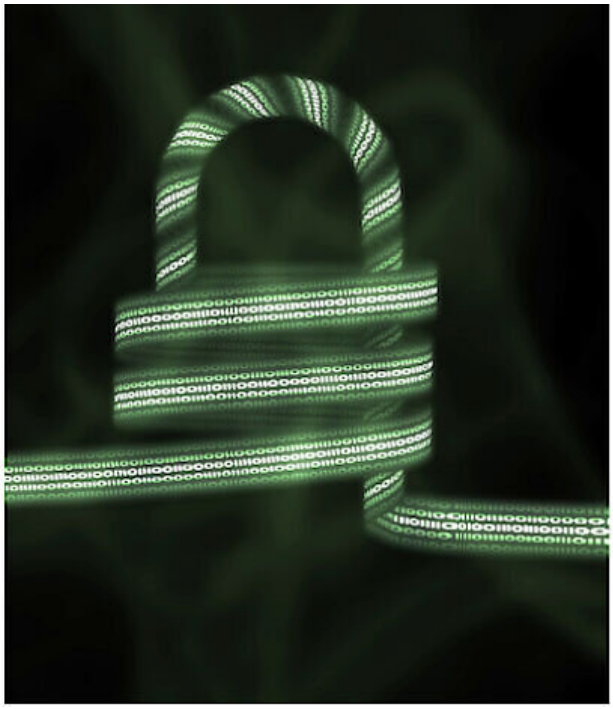
Quantum computing: When ignorance is wanted

February 18 2021



Artistic image of a homomorphic-encrypted quantum computation using a photonic quantum computer. Credit: Equinox Graphics, Universität Wien

Quantum computers promise not only to outperform classical machines in certain important tasks, but also to maintain the privacy of data processing. The secure delegation of computations has been an increasingly important issue since the possibility of utilizing cloud computing and cloud networks. Of particular interest is the ability to

exploit quantum technology that allows for unconditional security, meaning that no assumptions about the computational power of a potential adversary need to be made.

Different quantum protocols have been proposed, all of which make trade-offs between computational performance, security, and resources. Classical protocols, for example, are either limited to trivial computations or are restricted in their security. In contrast, homomorphic quantum encryption is one of the most promising schemes for secure delegated computation. Here, the client's data is encrypted in such a way that the server can process it even though he cannot decrypt it. Moreover, opposed to other protocols, the client and server do not need to communicate during the computation which dramatically boosts the protocol's performance and practicality.

In an international collaboration led by Prof. Philip Walther from the University of Vienna scientists from Austria, Singapore and Italy teamed up to implement a new quantum computation protocol where the client has the option of encrypting his input data so that the computer cannot learn anything about them, yet can still perform the calculation. After the computation, the client can then decrypt the output data again to read out the result of the calculation. For the experimental demonstration, the team used quantum light, which consists of individual photons, to implement this so-called homomorphic quantum encryption in a 'quantum walk' process. Quantum walks are interesting special-purpose examples of quantum computation because they are hard for classical computers, whereas being feasible for single photons.

By combining an integrated photonic platform built at the Polytechnic University of Milan, together with a novel theoretical proposal developed at the Singapore University of Technology and Design, scientist from the University of Vienna demonstrated the security of the encrypted data and investigated the behavior increasing the complexity

of the computations.

The team was able to show that the security of the encrypted data improves the larger the dimension of the quantum walk calculation becomes. Furthermore, recent theoretical work indicates that future experiments taking advantage of various photonic degrees of freedom would also contribute to an improvement in data security; one can anticipate further optimizations in the future. "Our results indicate that the level of security improves even further, when increasing the number of photons that carry the data," says Philip Walther and concludes "this is exciting and we anticipate further developments of secure quantum computing in the future."

The study is published in *npj Quantum Information*.

More information: Jonas Zeuner et al, Experimental quantum homomorphic encryption, *npj Quantum Information* (2021). DOI: 10.1038/s41534-020-00340-8

Provided by University of Vienna