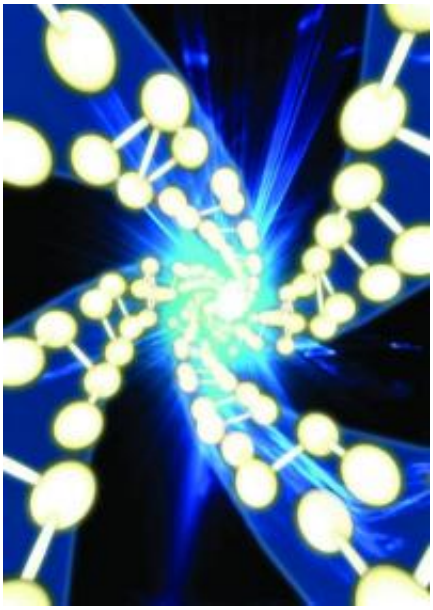
# Quantum mechanics enables perfectly secure cloud computing

January 19 2012



The image shows clusters of entangled qubits, which allow remote quantum computing to be performed on a server, while keeping the contents and results hidden from the remote server. Credit: EQUINOX GRAPHICS

Researchers have succeeded in combining the power of quantum computing with the security of quantum cryptography and have shown that perfectly secure cloud computing can be achieved using the principles of quantum mechanics. They have performed an experimental demonstration of quantum computation in which the input, the data processing, and the output remain unknown to the quantum computer. The international team of scientists will publish the results of the

experiment, carried out at the Vienna Center for Quantum Science and Technology (VCQ) at the University of Vienna and the Institute for Quantum Optics and Quantum Information (IQOQI), in the forthcoming issue of *Science*.

Quantum computers are expected to play an important role in future information processing since they can outperform classical computers at many tasks. Considering the challenges inherent in building quantum devices, it is conceivable that future quantum computing capabilities will exist only in a few specialized facilities around the world – much like today's supercomputers. Users would then interact with those specialized facilities in order to outsource their quantum computations. The scenario follows the current trend of cloud computing: central remote servers are used to store and process data – everything is done in the "cloud." The obvious challenge is to make globalized computing safe and ensure that users' data stays private.

The latest research, to appear in *Science*, reveals that quantum computers can provide an answer to that challenge. "Quantum physics solves one of the key challenges in distributed computing. It can preserve data privacy when users interact with remote computing centers," says Stefanie Barz, lead author of the study. This newly established fundamental advantage of quantum computers enables the delegation of a quantum computation from a user who does not hold any quantum computational power to a quantum server, while guaranteeing that the user's data remain perfectly private. The quantum server performs calculations, but has no means to find out what it is doing – a functionality not known to be achievable in the classical world.

The image shows multiple superimposed strings of data encoded in such a way that the quantum computation can be performed on a remote server, while still securely encrypted. Credit: EQUINOX GRAPHICS

The scientists in the Vienna research group have demonstrated the concept of "blind quantum computing" in an experiment: they performed the first known quantum computation during which the user's data stayed perfectly encrypted. The experimental demonstration uses photons, or "light particles" to encode the data. Photonic systems are well-suited to the task because quantum computation operations can be performed on them, and they can be transmitted over long distances.

The process works in the following manner. The user prepares qubits – the fundamental units of quantum computers – in a state known only to himself and sends these qubits to the quantum computer. The quantum computer entangles the qubits according to a standard scheme. The actual computation is measurement-based: the processing of quantum information is implemented by simple measurements on qubits. The user tailors measurement instructions to the particular state of each qubit and

sends them to the quantum server. Finally, the results of the computation are sent back to the user who can interpret and utilize the results of the computation. Even if the quantum computer or an eavesdropper tries to read the qubits, they gain no useful information, without knowing the initial state; they are "blind."

**More information:** "Demonstration of Blind Quantum Computing" Stefanie Barz, Elham Kashefi, Anne Broadbent, Joseph Fitzsimons, Anton Zeilinger, Philip Walther. DOI: 10.1126/science.1214707

Provided by University of Vienna