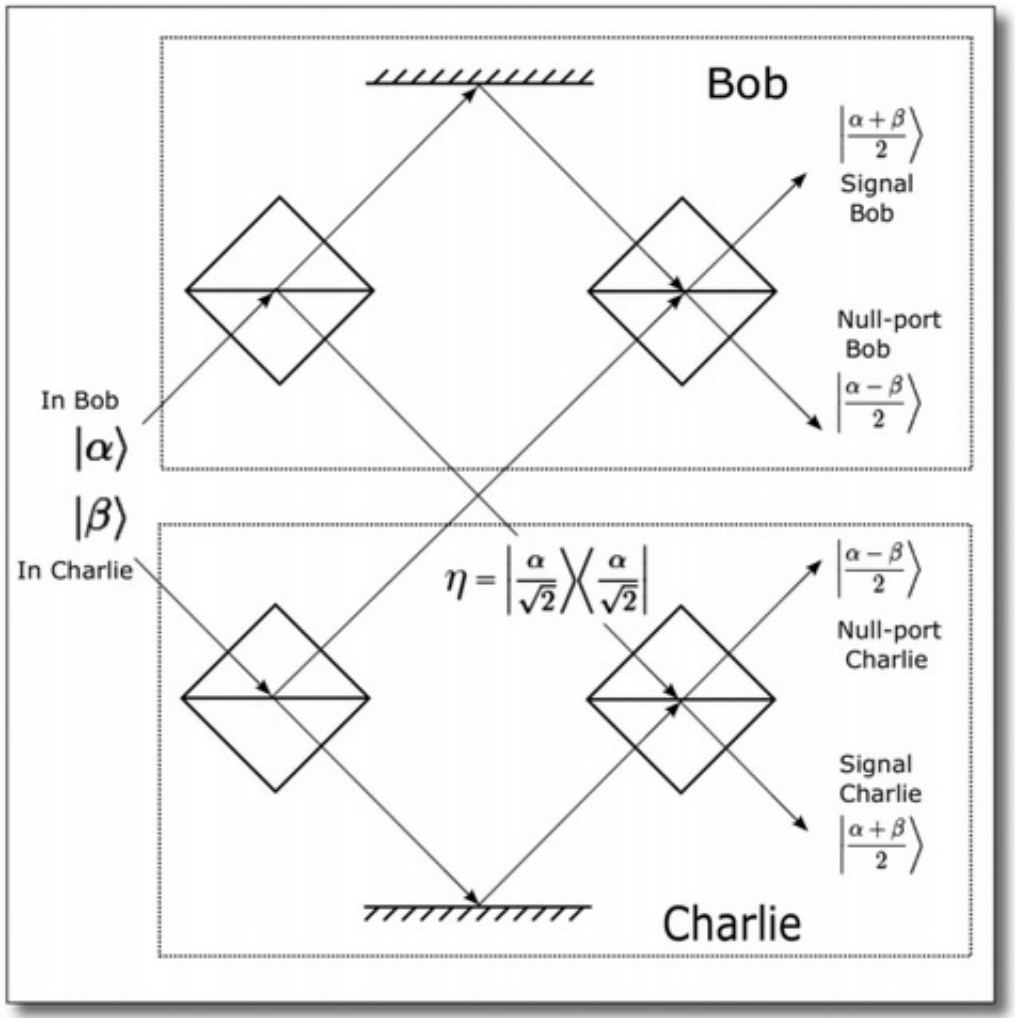
Quantum communication scheme provides guaranteed security without quantum memories

February 17 2014, by Lisa Zyga



A communication protocol that uses quantum digital signatures (QDS) offers security guaranteed by quantum mechanics. A new QDS protocol that does not require quantum memories is the first scheme that may be feasible with current

technology. Credit: Dunjko, et al. ©2014 American Physical Society

(Phys.org) —Quantum mechanics offers the potential for creating communication technologies with an inherently higher security level than today's classical technologies. Using quantum digital signatures (QDS), for example, messages can be sent to multiple recipients with the guarantee that the messages cannot be forged or tampered with.

"QDS provides essentially all features for which standard 'classical' digital signatures are used in modern communication—guaranteed authenticity, integrity and transferability of messages," Erika Andersson at Heriot-Watt University in Edinburgh, UK, told *Phys.org*. "The need for these features is ubiquitous in the modern e-world. They are used regularly in, for example, online banking, email systems, and smart electrical grids."

However, all QDS schemes proposed so far require advanced quantum memories capable of storing millions of qubits for months or even years. In contrast, today's state-of-the-art quantum memories cannot store information for longer than a few minutes, which makes all QDS schemes proposed so far unfeasible.

Now in a new paper published in *Physical Review Letters*, Andersson and UK-based coauthors Vedran Dunjko and Petros Wallden from Croatia and Greece, respectively, have proposed a QDS scheme that does not require any quantum memory, making the scheme feasible with current technology.

A generic QDS protocol consists of two stages: distribution and messaging. In the distribution stage, the sender sends pairs of quantum states—or quantum signatures—to multiple recipients. This stage is

independent of the future message sent in the messaging stage, where classical messages are sent to one or more recipients.

Sometimes, it may be months or years from the time the quantum signatures are sent to the time an actual message is sent, which is why quantum memories have been required.

The new protocol differs from the generic one in both stages. In the distribution stage, the quantum signatures are converted to classical information through quantum measurements, but they still retain the same level of security guaranteed by quantum mechanics. Yet because the information is now classical, it can be stored in a classical memory instead of a quantum one.

Similarly, in the messaging stage, only classical data is processed by the receivers. One receiver may authenticate a message received directly from the sender, and a second receiver may verify a message forwarded by the first receiver. The scientists showed that, in both cases—authentication and verification—the new scheme provides security against problems such as forgery, tampering, and repudiation (in which the second receiver rejects the forwarded message).

By showing that it is possible to perform a QDS scheme by using classical correlations, while maintaining the same security that is guaranteed by quantum correlations, the results open the doors to the experimental realization of QDS systems.

"We have, since the publishing of our work, already carried out an experimental demonstration of our scheme on a small scale, in collaboration with the group of Prof. Gerald Buller at Heriot-Watt University," the physicists wrote. "This we also aim at extending. Furthermore, we are developing new theoretical results which will make QDS even more efficient and feasible—everything can always be

improved!"

More information: Vedran Dunjko, et al. "Quantum Digital Signatures without Quantum Memory." *Physical Review Letters*. DOI: 10.1103/PhysRevLett.112.040502

Robert J. Collins, et al. "Optical realisation of Quantum Digital Signatures without quantum memory." **arXiv:1311.5760 [quant-ph]**