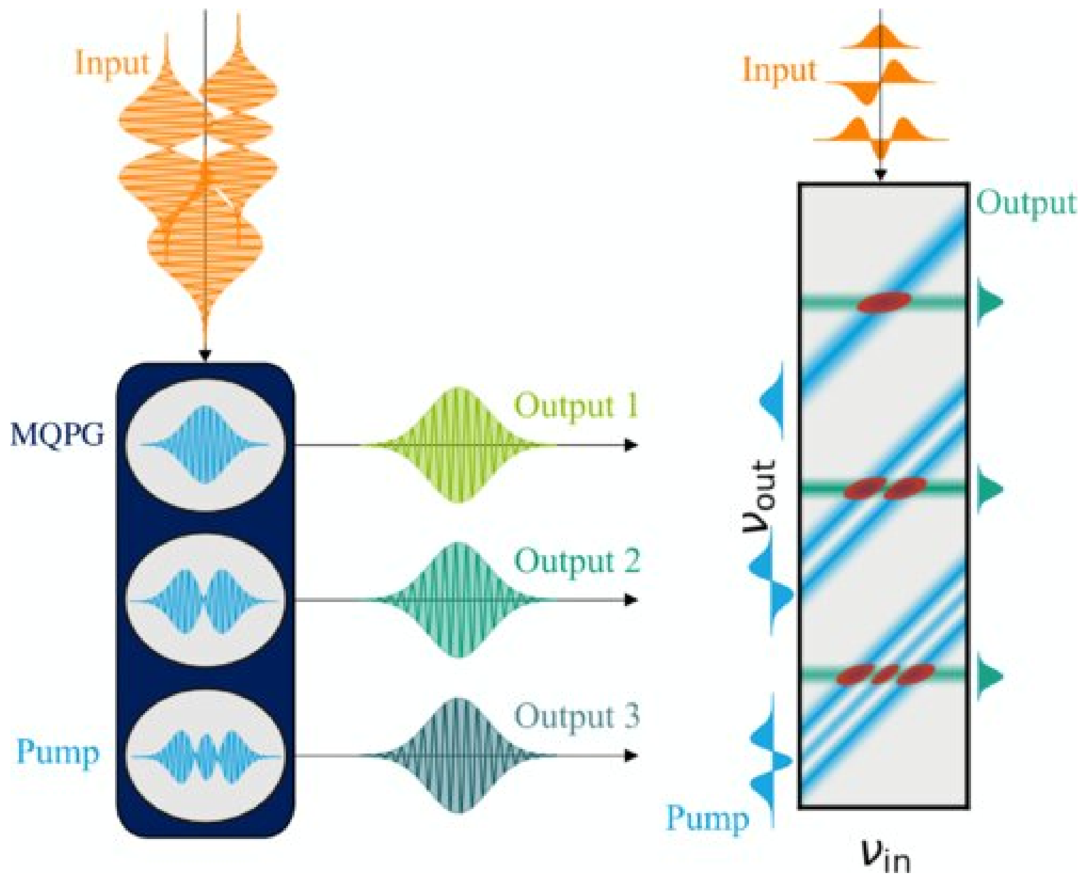
New technology developed for quantum cryptography applications

May 10 2023



The working principle of the MQPG (left) and description in frequency space (right): in the MQPG waveguide, the input photons (orange) are demultiplexed to different output frequencies (green) on the basis of their TM. The TMs to be measured are selected by shaping the pump field (blue). Credit: *PRX Quantum* (2023). DOI: 10.1103/PRXQuantum.4.020306

The development of quantum computing means that the use of classic cryptography for secure communications is in danger of becoming obsolete. Quantum cryptography, on the other hand, uses the laws of quantum mechanics to ensure total security. One example of this is quantum key distribution, which enables two parties to secure a message via a random secret key.

This is generated by quantum particles, generally photons. To achieve this, researchers are increasingly making use of an alphabet based on particular characteristics of photons, namely their color composition. However, previously no equipment had been created to decode the information again. Researchers at Paderborn Universities have now developed such a decoder and have published their results in the journal *PRX Quantum*.

"Quantum key distribution protocols using binary code are widespread. However, their security and efficiency could be improved by using a larger alphabet for coding. This involves using what are known as temporal pulse modes in which information is coded into photons' color composition. A key distribution system using this method requires a multi-channel decoder able to 'read' every letter of an alphabet at once. No such device had previously been created," explains Dr. Benjamin Brecht, a physicist at Paderborn University.

Paderborn's researchers have now developed a multi-output quantum pulse gate (mQPG). It separates the incoming letters into various output colors that the physicists can identify using a spectrometer. They have also demonstrated a complete, high-dimensional mQPG-based decoder that enables encryption protocols based on individual photons. "The versatility of mQPG makes it a valuable resource for numerous applications in quantum communications, and also opens up other opportunities for all technologies based on temporal modes," Brecht notes.

More information: Laura Serino et al, Realization of a Multi-Output Quantum Pulse Gate for Decoding High-Dimensional Temporal Modes of Single-Photon States, *PRX Quantum* (2023). [DOI: 10.1103/PRXQuantum.4.020306](https://doi.org/10.1103/PRXQuantum.4.020306)

Provided by Universität Paderborn