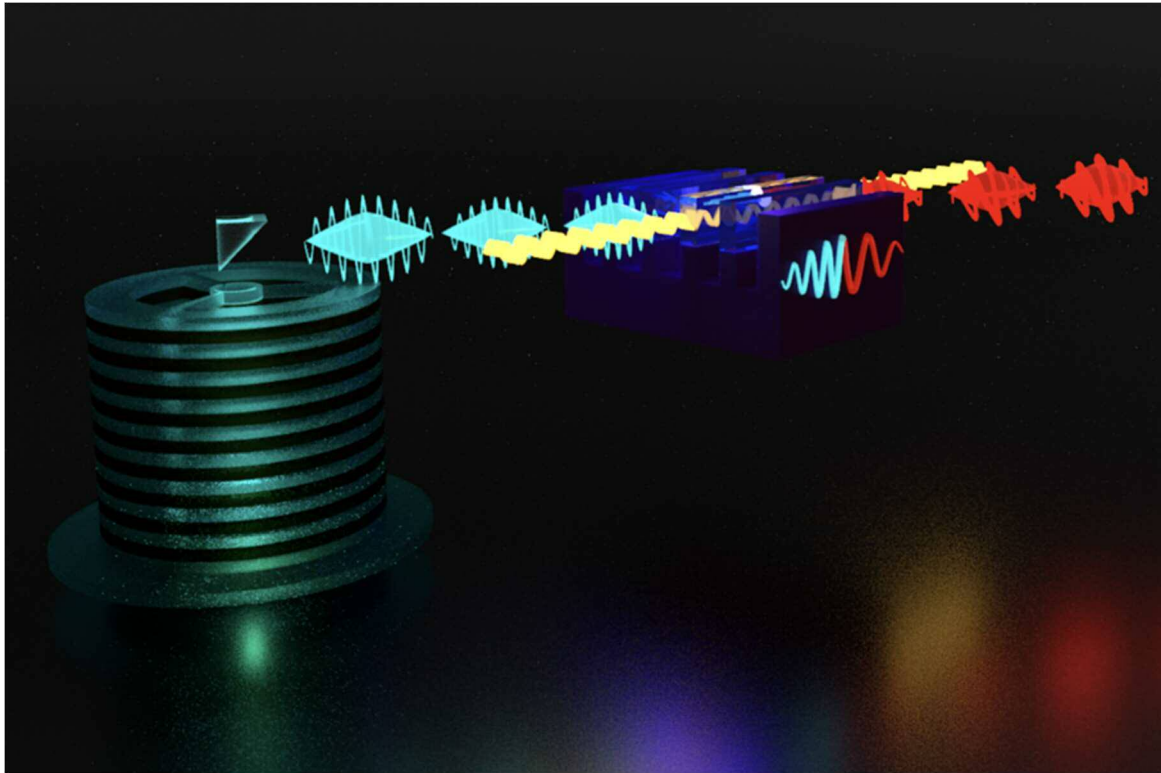


PRESS RELEASE: Quantum Nanomaterials Achieve Breakthrough Encryption Performance Over Conventional Optical Fibre



A group of researchers from Scottish Universities working alongside international collaborators have achieved remarkable new results in quantum secure encryption over standard optical-fibre networks. The results were published in *Nature Communications*. Led by Heriot-Watt and involving researchers from the Universities of Strathclyde, California and Leiden, the collaboration focused on the potential of ‘quantum dots’ – semiconductor nanostructures that behave like artificial atoms – to act as single-photon sources.

Quantum light sources that emit very faint signals are an essential component for achieving encrypted communications via quantum secure methods. Quantum dot single-photon sources have the additional advantage of being compatible with so-called quantum memories, a key enabling technology towards the establishment of a future quantum internet.

To date, though, this potential has been limited by practical performance issues, such as distance limitations due to photon loss in optical fibres, and unfeasibly long processing times to generate secure keys from real-world data.

The results of this new work overcome these limitations, achieving record key rates and distance results by converting the photons from a high-quality quantum dot to wavelengths used in low-loss telecom networks.

A major development is a new security analysis of the amount of secure key distillable from practical amounts of raw data. Using techniques also utilised in satellite quantum communications, the researchers showed that they could generate robust encryption keys

for fibre distances of up to 175km in just an hour, when previously achieving this kind of security guarantee over such length of fibre would have taken decades.

The feasibility study that led to this experimental demonstration was originally funded by the [EPSRC Quantum Communications Hub project](#), that aims to develop and implement next generation quantum secure networks at all distance scales. These new results convincingly establish that the use of frequency-converted quantum dots is possible at high rates and encryption key acquisition times, relevant for metropolitan-scale quantum communications networks over conventional optical fibre. This breakthrough brings single-photon-based quantum security much closer to practical technology and application.

Prof Alessandro Fedrizzi, lead researcher at Heriot-Watt University, said, “Generating quantum keys with single photon sources is challenging, but the high rates and distances we have achieved show that this is a very competitive technology that is also future-proof for quantum networks.”

University of Strathclyde’s Dr Daniel Oi, who led the secure key generation analysis said – “The work demonstrates the benefits of close collaboration between experimentalists and theorists. We utilised recent advances in security analysis, suitably adapted for imperfect single photon sources, and achieved drastic improvements over hitherto standard methods.”

Journal: Nature Communications

DOI: [10.1038/s41467-023-39219-5](https://doi.org/10.1038/s41467-023-39219-5)

Article title: “Single-emitter quantum key distribution over 175 km of fiber with optimised finite key rates”

Article publication date: 16 June 2023