

Chip-Integrated Quantum Digital Signature Network Achieves High-Rate Performance

GA, UNITED STATES, March 27, 2025 /EINPresswire.com/ -- Quantum digital signatures (QDS) offer an information-theoretically secure solution for ensuring data integrity, authenticity, and non-repudiation. To address the challenges faced by QDS in its practical implementation, including high costs, large sizes, and low signature rates, Chinese scientists have proposed and validated a chip-integrated quantum signature network. Experimental results surpass all current state-of-the-art QDS experiments. This research paves the way for the large-scale deployment of quantum networks.

In the context of traditional encryption technologies facing the threat of quantum computing, quantum communication has attracted significant attention due to its unique advantages in information security.

[Quantum Digital Signature](#) (QDS), as a core cryptographic technique, ensures integrity, authenticity, and non-

repudiation of information transmission, with important applications in e-commerce, digital currencies, and blockchain. Currently, QDS has rapidly grown from proof-of-concept to mature demonstrations, and it is expected to become the next commercial quantum cryptographic technology. However, all previous QDS systems have relied on expensive and bulky optical equipment, which pose challenges for large-scale deployment and seamless integration with existing communication infrastructures. Therefore, the development of a low-cost, high-rate, and easily scalable chip-based QDS network holds significant research value and practical application potential.

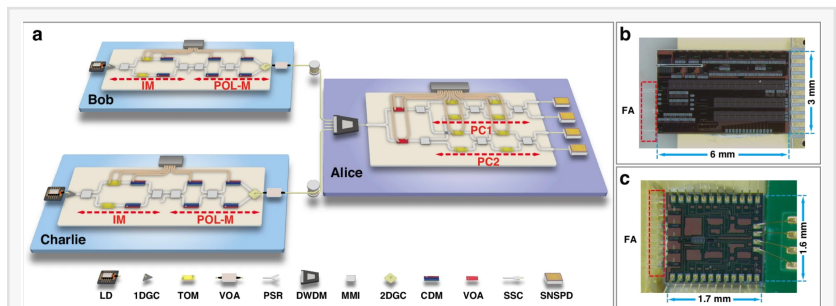


Figure 1. Experimental setup.

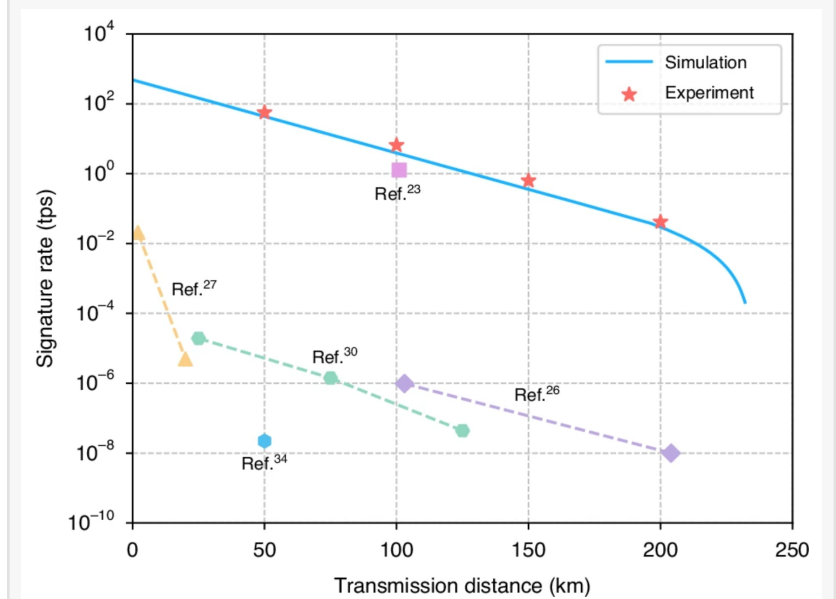


Figure 2. Simulation and experimental signature rates under different transmission distances.

In a new paper published in *Light Science & Applications*, a team of scientists led by Professor Kejin Wei from Guangxi University, Xi Xiao from the National Information Optoelectronics Innovation Center (NOEIC), and Professor Hua-Lei Yin from Renmin University of China proposed an innovative star-topology QDS network architecture and developed a 1-decoy-state one-time universal hash-QDS protocol that not only improves the signature rate but also significantly reduces the complexity of system hardware and data post-processing. A three-node network was subsequently constructed using silicon-based encoder and decoder chips for experimental verification. The experimental results surpass those of all current advanced QDS experiments. This study validates the feasibility of chip-based QDS, thereby paving the way for large-scale deployment and integration with existing fiber infrastructure.

The proposed QDS network utilizes star topology and consists of three main components: terminal users, optical switches, and integrated measurement units (IMUs). Each terminal user is equipped with a compact transmitter chip connected to a central node containing several IMUs. The IMUs include quantum state decoding chips, single-photon detectors, and personal computers. Prof. Kejin Wei highlighted one main advantage of this QDS network architecture:

"First, each user requires only a compact transmitter chip fabricated using integrated platforms. Second, the signer maintains the expensive and bulky measurement system, which is shared by all terminal node users, thus eliminating the need for integrating SPDs on a chip, as users do not need to perform quantum detection. Third, this network architecture can easily integrate into existing classical telecommunications infrastructure and is compatible with the current quantum network by flexibly configuring the IMU".

Prof. Hua-Lei Yin added: "In order to enhance performance and compatibility with chip-based network structures, we developed a modified QDS protocol. By using a one-time universal hash function to generate a fixed-length digest representing the document's features and incorporating advanced security proofs, the protocol enables the signing of arbitrarily long documents using imperfectly pre-distributed keys. This improvement is essential for the practical deployment of QDS networks. Notably, our protocol significantly reduces computational costs and latency during the post-processing phase".

To validate the proposed network, the research team developed a three-node chip-based QDS network to demonstrate its operation. To demonstrate the progress entailed by this work, the researchers compared the experimental results obtained with current state-of-the-art QDS experiments. The proposed chip-based QDS scheme is shown to significantly improve the signature rate. Notably, at a distance of 200 km, a signing rate of 0.04 times per second was achieved when signing a 1 Mbit file.

"This research not only advances the practical implementation of QDS technology but also holds great potential for applications in other quantum communication fields, such as quantum e-commerce and quantum blockchain." Prof. Kejin Wei forecast.

References

DOI

[10.1038/s41377-025-01775-4](https://doi.org/10.1038/s41377-025-01775-4)

Original Source URL

<https://doi.org/10.1038/s41377-025-01775-4>

Funding information

This study was supported by the National Natural Science Foundation of China (Nos. 12274223, 62171144, 62031024, and 62171485), the Guangxi Science Foundation (No.2021GXNSFAA220011), the Open Fund of IPOC (BUPT) (No. IPOC2021A02) and the Innovation Project of Guangxi Graduate Education (No. YCBZ2024002).

Lucy Wang

BioDesign Research

[email us here](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/797619135>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2025 Newsmatics Inc. All Right Reserved.