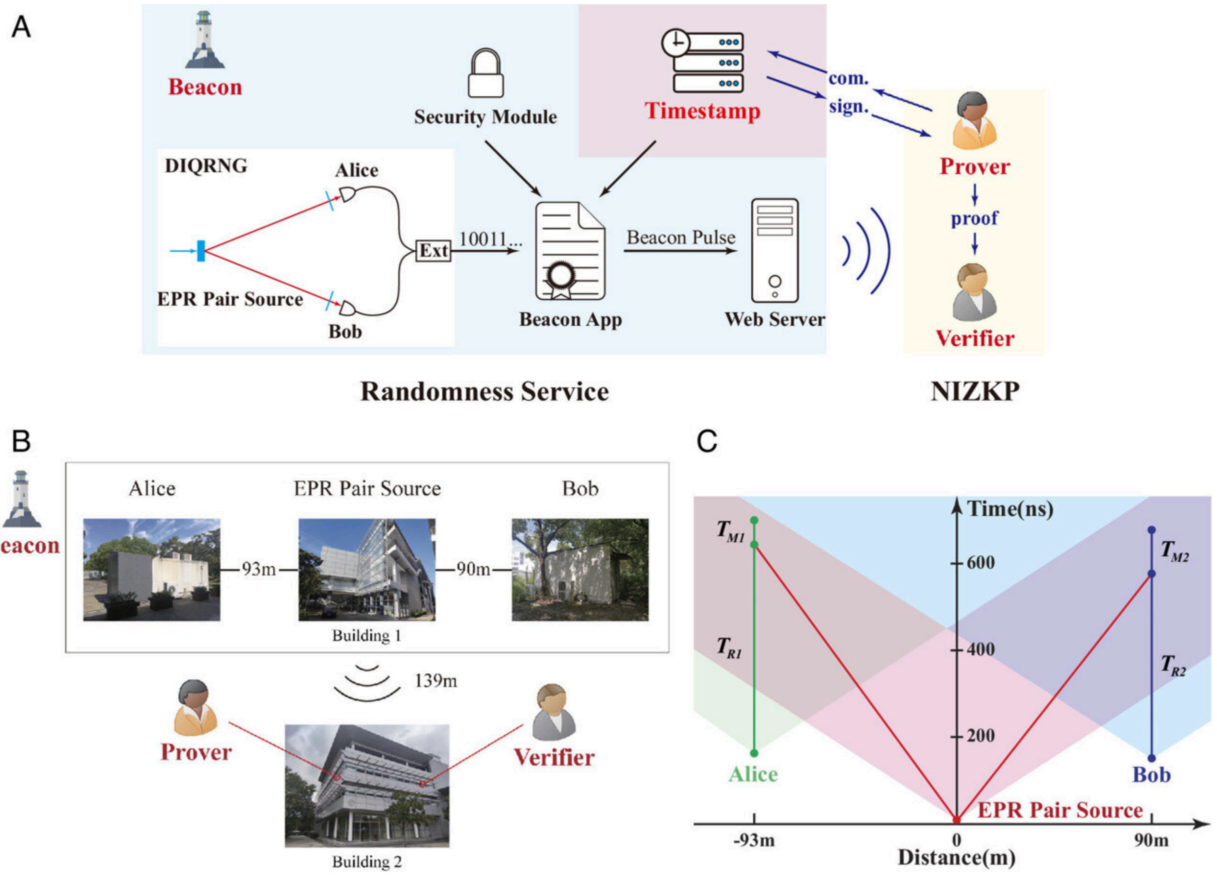
PHYS.ORG

# Researchers achieve zero-knowledge proof based on device-independent quantum random number beacon

November 21 2023, by Liu Jia



Schematics of the experiment. Credit: *Proceedings of the National Academy of Sciences* (2023). DOI: 10.1073/pnas.2205463120. *Proceedings of the National Academy of Sciences* (2023). DOI: 10.1073/pnas.2205463120

Zero-knowledge proof (ZKP) is a cryptographic tool that allows for the verification of validity between mutually untrusted parties without disclosing additional information. Non-interactive zero-knowledge proof (NIZKP) is a variant of ZKP with the feature of not requiring multiple information exchanges. Therefore, NIZKP is widely used in the fields of digital signature, blockchain, and identity authentication.

Since it is difficult to implement a true random number generator, deterministic pseudorandom number algorithms are often used as a substitute. However, this method has potential security vulnerabilities. Therefore, how to obtain true random numbers has become the key to improving the security of NIZKP.

In a study published in *PNAS*, a research team led by Prof. Pan Jianwei and Prof. Zhang Qiang from the University of Science and Technology of China (USTC) of the Chinese Academy of Sciences, and the collaborators, realized a set of random number beacon public services with device-independent quantum random number generators as entropy sources and post-quantum cryptography as identity authentication.

The researchers built a beacon public service system based on a device-independent quantum random number generator (DIQRNG). The system could broadcast generated random numbers to the public in real-time, ensuring the security of the random numbers during the broadcast process.

To ensure the security of the broadcast process, the researchers adopted a quantum secure signature algorithm that could resist quantum attacks. The algorithm guaranteed the integrity and authenticity of the random number during transmission.

By utilizing the received random numbers from DIQRNG, they constructed and experimentally verified a more secure NIZKP protocol.

The new protocol was able to eliminate potential security hazards and further improved the security of NIZKP.

This study was the first to combine three different fields: quantum nonlocality, quantum secure algorithm, and zero-knowledge proof, and significantly improved the security of zero-knowledge proofs, in which the constructed public-facing random number service has important potential applications in fields such as cryptography, the lottery industry, and social welfare.

In the future, with the continuous development and application of quantum technology, it is expected to see more innovative solutions based on the principles of quantum mechanics, which will provide strong support for solving the challenges in the field of information security.

**More information:** Cheng-Long Li et al, Device-independent quantum randomness–enhanced zero-knowledge proof, *Proceedings of the National Academy of Sciences* (2023). DOI: 10.1073/pnas.2205463120

Provided by Chinese Academy of Sciences

Citation: Researchers achieve zero-knowledge proof based on device-independent quantum random number beacon (2023, November 21) retrieved 28 April 2024 from https://phys.org/news/2023-11-zero-knowledge-proof-based-device-independent-quantum.html