# Testing the Security of Quantum Key Distribution

**Bell nonlocality is insufficient to ensure the security of a type of secure quantum-communications protocol known as DI-QKD.**

By **Christopher Crockett**

A type of secure quantum communications protocol known as device-independent quantum key distribution (DI-QKD) uses peculiarities of quantum mechanics to generate its message-encryption keys. These keys can be shared by end users over public channels while remaining impervious to eavesdroppers, even over an untrusted network. Now, an analysis shows that one previously established requirement for DI-QKD—known as "Bell nonlocality"—fails to keep some DI-QKD protocols secure [**1**]. The team says that the finding could help researchers identify vulnerabilities in quantum encryption methods.

In DI-QKD, a device produces pairs of entangled particles and then separates them, sending one particle to one party and the other particle to another. Both parties then use different devices to make independent measurements on the particles that they receive. The parties know nothing about any of the devices involved in this process—all of which could, in principle, be imperfect or even malicious. For the devices to be suitable for DI-QKD, the measurement outcomes must exhibit correlations that defy classical description; that is, they must be "nonlocal."

Credit: Tony Craddock/stock.adobe.com

To test whether this requirement is sufficient for unbreakable encryption, Máté Farkas of the Institute of Photonic Sciences, Spain, and colleagues subjected the most commonly studied DI-QKD protocols to a simple attack. An unsavory actor sets up all the devices so that a small fraction of the particles behaves deterministically when measured. The observed correlations will still be nonlocal to honest users, but the eavesdropper will know the outcomes for some measurements, allowing them to break the encryption code. The team shows that such an attack can render the protocols they studied unsecure.

Christopher Crockett is a freelance writer based in Arlington, Virginia.

## REFERENCES

1. M. Farkas *et al.*, "Bell nonlocality is not sufficient for the security of standard device-independent quantum key distribution protocols," **Phys. Rev. Lett. 127, 050503 (2021).**