Research Directions: Quantum Technologies

www.cambridge.org/qut

Question

What are the full capabilities of relativistic quantum cryptography?

Carl A. Miller

Computer Security Division, National Institute of Standards and Technology, Gaithersburg, MD, USA

Cite this article: Miller CA (2023). What are the full capabilities of relativistic quantum cryptography? *Research Directions: Quantum Technologies*. **1**, e6, 1. https://doi.org/10.1017/qut.2022.4

Received: 29 July 2022
Accepted: 1 August 2022

Author for correspondence:
Carl A. Miller,
Email: carl.miller@nist.gov

Quantum cryptography bases its security proofs on physical assumptions. A longstanding observation in the field is that we may be able to do more cryptographic tasks when we assume not only the laws of quantum mechanics but also the impossibility of superluminal signaling (i.e., that information cannot travel faster than the speed of light). Relativistic quantum cryptography takes into account the spatial locations of the parties involved and uses the impossibility of superluminal signaling as a basis for security. Previous efforts in this field have been fruitful, both theoretically and experimentally.

The goal of this research direction is to map out the full range of cryptography that can be carried out in a relativistic quantum setting. Two important threads are:

1. How can relativistic quantum cryptography be used to improve the security of positioning, navigation, and timing technologies?
2. How can relativistic quantum cryptography be used to better accomplish cryptographic tasks in a two-party setting (such as coin flipping, bit commitment, and oblivious transfer)?

Research Directions

CAMBRIDGE UNIVERSITY PRESS