CP-08-03

Quantum communication beyond QKD: Position-based cryptography

Harry Buhrman

Quantinuum

Abstract

On 20 July 1969, millions of people held their breath as they watched, live on television, Neil Armstrong set foot on the Moon. Yet Fox Television has reported that a staggering 20% of Americans have had doubts about the Apollo 11 mission. Could it have been a hoax staged by Hollywood studios here on Earth? Position-based cryptography may offer a solution. This kind of cryptography uses the geographic position of a party as its sole credential. Normally digital keys or biometric features are used.
A central building block in position-based cryptography is that of position verification. The goal is to prove to a set of verifiers that one is at a certain geographical location. Protocols typically assume that messages cannot travel faster than the speed of light. By responding to a verifier in a timely manner one can guarantee that one is within a certain distance of that verifier. It was shown that position-verification protocols only based on this relativistic principle can be broken by attackers who simulate being at the claimed position while physically residing elsewhere in space.
Because of the no-cloning property of quantum information (qubits) it was believed that with the use of quantum messages one could devise protocols that were resistant to such collaborative attacks. Several schemes were proposed that later turned out to be insecure. In 2012 it was shown that also in the quantum case no unconditionally secure scheme is possible. However, many questions concerning the optimality of the attack remain open.
We will review the old results as well as some of the new sometimes very surprising connections with seemingly unconnected research areas such as holography, ADS/CFT correspondence, and classical primitives like

conditional disclosure of secrets (CDS), secure message passing (SMP), and functional analysis. We will also cover some of the recent proposals for implementing position verification protocols that are secure when the attackers have a limited amount of entanglement.