

# Quantum key distribution

- Secure communication based on laws of nature -

## Motivation

When we exchange some information over phone or internet, we always encounter a risk of being eavesdropped. i.e., unauthorized parties might obtain some knowledge on the information.

By making use of mysterious laws of nature, which is called quantum mechanics, we are working on problems how we can prevent eavesdropping.

## Originality

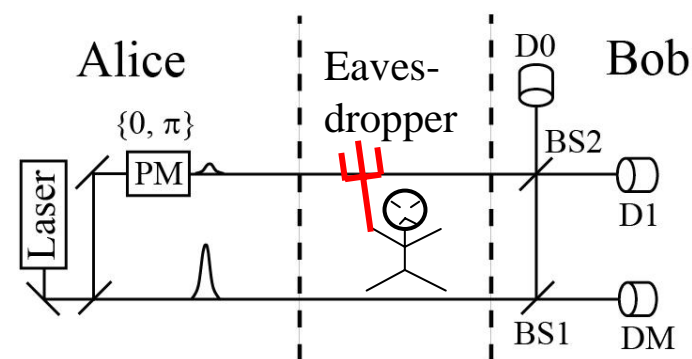
We have rigorously proven that B92 quantum key distribution protocol, proposed by Bennett in 1992, is secure not only against a particular eavesdropping, but also against any eavesdropping on communication lines.

## Impact

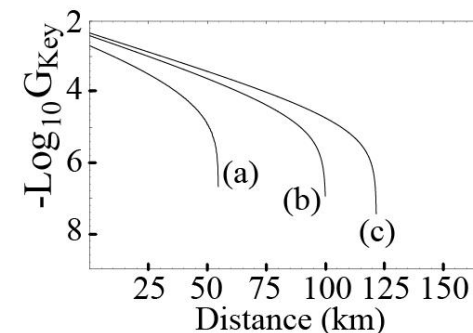
If quantum key distribution is available for commercial use, we will live in a society where important information such as credit card information can be exchanged via communication lines without any risk of information leakages to unauthorized parties.

Contact person: Dr. Kiyoshi Tamaki  
Optical Science Laboratory, NTT Basic Research Laboratories  
TEL: 046-240-3417 FAX: 046-240-4726  
e-mail: tamaki@will.brl.ntt.co.jp

### B92 Quantum Key Distribution



### Secure communication distance and communication capacity per pulse ( $G_{\text{key}}$ )



We can achieve about 125km of communication distance by appropriately choosing the experimental parameters.