HUMBOLDT-UNIVERSITÄT ZU BERLIN
INSTITUT FÜR PHYSIK

Sonderkolloquium

Freitag, 7. Oktober 2016, 14:00 Uhr

Prof. Dr. Mladen Pavičić

Center of Excellence for Advanced Materials and Sensing Devices (CEMS), Photonics and Quantum Optics Unit, Ruđer Bošković Institute, Zagreb, Croatia

"Two-Way Deterministic Communication Is Like Sending Plain Text under Quantum Protection"

Abstract:
We present an attack on two-way quantum key distribution protocols in which Alice encodes messages so as to change the states of qubits she receives from Bob and then sends them back to him. In the attack, an undetectable Eve sends decoy qubits to Alice to encode them, copies all Alice's encoding onto Bob's delayed qubits and sends them back to him. For it, we show that there is no critical Eve's disturbance, that the mutual information between all parties is always constant, and that the recent unconditional security for a single photon two-way protocol cannot be considered proved.

Ort: Vortragsraum 007

IRIS Adlershof
Humboldt-Universität zu Berlin
Zum Großen Windkanal 6
12489 Berlin