Setting A Disordered Password on A Photonic Memory

Wen Te Liao
Dept. of Physics, NCU

In this talk we will talk about an all-optical method of how to set a disordered password on different schemes of photonic memory. While photons are regarded as ideal information carriers, it is imperative to implement such data protection on all-optical storage. However, we wish to address the intrinsic risk of data breaches in existing schemes of photonic memory. We theoretically demonstrate a protocol using spatially disordered laser fields to encrypt data stored on an optical memory, namely, encrypted photonic memory. To address the broadband storage, we also investigate a scheme of disordered echo memory with a high fidelity approaching unity. The proposed method increases the difficulty for the eavesdropper to retrieve the stored photon without the preset password even when the randomized and stored photon state is nearly perfectly cloned. Our results pave ways to significantly reduce the exposure of memories, required for long-distance communication, to eavesdropping and therefore restrict the optimal attack on communication protocols. The present scheme also increases the sensitivity of detecting any eavesdropper and so raises the security level of photonic information technology.