Alberto Dall'Arche

Department of Information Engineering, University of Padova
Via Gradenigo 6/b - 35131 Padova, Italy
alberto.dallarche@dei.unipd.it

Experimental demostration of B92 protocol with non-maximally entangled photons

A. Dall'Arche, M. Tomasin, M. Lucamarini, G. Vallone, P. Villoresi

In 1992 Charles Bennet proposed his famous protocol B92 for quantum key distribution (QKD) that was proven to be unconditionally secure, nonetheless this protocol can suffer of the unambiguous state discrimination. Many implementations and improvements were proposed using the typical prepare and measure (PM) scheme, only recently was presented an entangled-based scheme that exploit non-maximally entangled states, named ent-B92.
This implementation of the B92 protocol gives many advantages with respect to the standard PM scheme, on the security side, which is no more based on efficiency measurements but on violation of the Bell inequality. Taking into account a real scenario with untrusted devices, the ent-B92 protocol is better than other QKD protocols because it lowers the efficiency of the so called "detection loophole".
Here we would propose the feasibility demonstration of the ent-B92. Our setup consists of a pulsed laser that pumps a type I SPDC crystal which generates non-maximally entangled photons. The transmitter and the receiver were implemented with linear polarizers and retarders to perform a complete state tomography.
Several proofs were taken maximizing the secret key rate and minimizing the QBER. Our results prove the feasibility of the ent-B92 protocol and show the improvements with respect to the BB84 QKD protocol.