Security proof of improved-SARG04 protocol using the same four qubit states

ABSTRACT

We propose a security proof for a new class of quantum key distribution protocol namely Improved-SARG04. This protocol differs from BB84 and SARG04 protocol in the sifting process and provably outperforms those protocols against Photon Number Splitting attack at zero error, with secure transmission distance of 125 km of SSMF.

Keyword: Quantum key distribution; Photon number splitting (PNS)