

Long Range Secure Key Distribution Over Multiple Amplified Fiber Spans Based on Environmental Instabilities

Ben Wu^{1,2}, Yue-Kai Huang¹, Shaoliang Zhang¹, Bhavin J. Shastri², Paul R. Prucnal²

²*Lightwave Communications Research Laboratory, Department of Electrical Engineering,
Princeton University, Princeton, NJ 08544, USA
benwu@princeton.edu*

Abstract: Using environmental instability induced signal phase fluctuation, we demonstrated a secure key distribution system over a 240-km bidirectional fiber-pair link. The scheme is compatible with commercial WDM systems and optical amplifiers for long-range transmissions.

OCIS codes: (060.2330) Fiber optics communications; (060.4785) Optical security and encryption.

1. Introduction

Network security relies on data encryption between signal transmitters and receivers. The basis of data encryption is to generate and distribute secure “keys”. Quantum key distribution (QKD) has been widely studied as a secure key distribution system [1]. Compared with software based key distribution, QKD has the advantage that if the eavesdropper records the wrong quantum state, the original signal is lost and changed, and the eavesdropper cannot use post-processing techniques to recover it. Although QKD has been demonstrated to be secure, its deployment has practical issues. First, a QKD system requires single photon transmission, which means it is not compatible with optical networks with optical amplifiers. Second,

