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

**Ben Wu[1,2], Yue-Kai Huang[1], Shaoliang Zhang[1], Bhavin J. Shastri[2], Paul R. Prucnal[2]**
[1]*NEC Laboratories America, Inc., Princeton, NJ 08540, USA*
[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, to be compatible with public WDM channels, the single photon channel requires specially designed filters with high isolation ratio, which increases the complexity of the system design and implementation.

In this paper, we demonstrate a key distribution scheme that is compatible with both optical amplifiers for long-range transmission and public WDM systems without specially designed filters. The key is generated via fiber index fluctuation induced by environmental instabilities, including temperature changes and mechanical vibrations [2]. Each of the communicating pair employs an interferometer with long optical delay to convert the combined environmental instabilities to phase signals. Broadband sources are used as the signal carrier to improve system security by minimizing signal coherence length. The key distribution scheme was verified in a 240-km long WDM link, achieving a key-rate of 100 bps and pre-coded key error rate of $5\times10^{-3}$.

## 2. Experimental setup and principle

The experimental setup is shown in Fig. 1. The key signal is derived from phase fluctuations in two Mach-Zehnder (MZ) fiber interferometers at both ends of a transmission system. It is transmitted together with 38 standard public channels through a 240-km fiber-pair link with multiple amplifiers. Since the signals in both directions go through the same physical paths, the resulting interference at the MZI outputs will be the same, making key sharing possible. Broadband sources are used as the signal carriers to prevent the eavesdropper from measuring the phase directly with coherent detection. In the experiment, both Alice and Bob use filtered amplified spontaneous emission (ASE), having 150GHz bandwidth and 1547.6nm center wavelength, as the light source. Since the broadband source has short coherence length, the optical delay between Alice ($L_1$) and Bob ($L_2$) has to be matched to within a few millimeters to recover the phase information [3]. The optical delays used are typically in the range to tens of kilometers, making it extremely difficult for the eavesdropper to scan the optical delay and to find the coherence length in mm resolution.

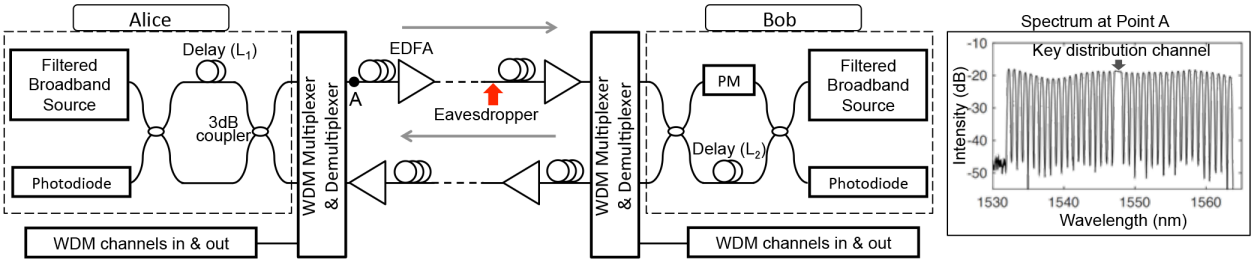


Fig. 1. Experimental setup. The inset shows the spectrum at point A of the setup (EDFA: erbium doped fiber amplifier; WDM: wavelength division multiplexer; PM: phase modulator)

## 3. Experiment results and analysis

The optical delays created by Alice's and Bob's MZIs are 26-km. The optical delay has to be long enough to prevent the eavesdropper from using coherent detection to measure the fringes of the spectrum and calculating the length of the optical delay. A long optical delay requires high spectral resolution to observe the fringes. To achieve the high spectral resolution, the eavesdropper needs to collect the temporal data in a relatively long period of time. During the time of the data collection, the phase can change and will essentially smear out measurement results. To emulate the eavesdropper (red arrow in Fig. 1), we perform a coherence detection attack on the system using an ultra-stable fiber laser with 400-Hz linewidth as local oscillator. When different optical delays are tested, as shown in Fig. 2, it is found that it is not secure to use delay length below 10-km.

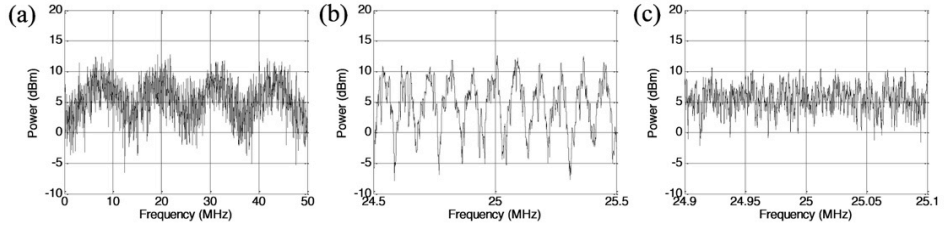


Fig. 2. Spectra taken from interferometer output using coherent detection (a) Delay = 20m (b) Delay = 2.3km (c) Delay = 26km

The rapidly changing phase protects the signal against coherent detection. However, for signal synchronization between Alice and Bob, the rapid change has to be filtered. The phase change needs to be slow enough that the signals in the two opposite directions experience the same phase changes. To remove the high frequency component of the phase signal, the received interference results need to be converted back to phase information. We use a phase modulator that switches between 90° and 0° at a rate of 100kHz. This is more than 10 times faster than the rate of the phase change. In this case, both sine and cosine of the phase can be measured and the original phase can be recovered (Figs. 3 (a) and (b)). A low pass filter with a 3dB cutoff frequency of 62.5Hz is applied to the phase signal. Figs. 3 (c) and (d) show matching results from the cosine functions of the two filtered phase signals. The self-correlations of Alice's and Bob's cosine functions are plotted in Fig. 3(e), showing true temporal randomness of the generated key. They are also highly correlated. Cross-correlation reaches 0.8. The key sequence is digitized from both the sine and cosine functions of the phase. By optimizing the threshold of digitization, the key generation achieves a rate of 100bps with an error rate of $5\times10^{-3}$, which can be corrected using a hard decision FEC technique [4], and key reconciliation [5].

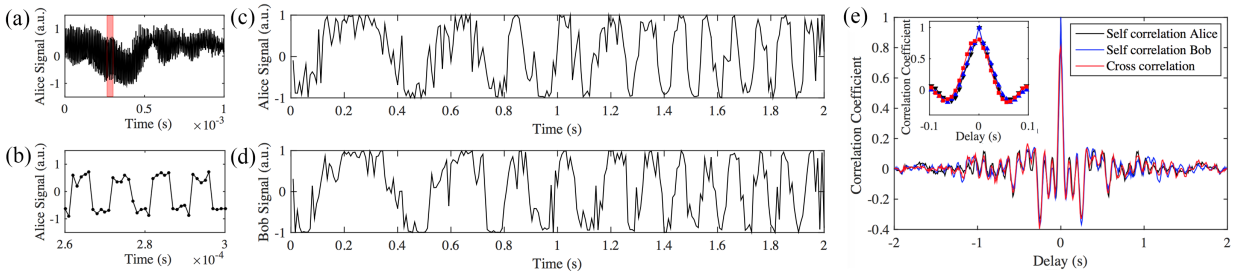


Fig. 3. (a) and (b) are signal with phase modulator (b) is the enlarged view of the red region in (a), (c) and (d) are Alice and Bob signals after the high frequency components are filtered, (e) is the correlation of the signals, the inset in (e) is the enlarged view, when delay is close to zero.

## 4. Conclusion

We proposed and experimentally demonstrated a key distribution system based on environmental instabilities. The signal can be amplified by EDFAs and 240km bi-direction transmission is demonstrated. The key distribution channel shares the C-band transmission spectrum with 38 neighboring WDM channels. The system generates a key at a rate of 100bps with an error rate of $5\times10^{-3}$. The coherence length of the wide-band ASE source as well as the fast phase fluctuation from the long optical delay safeguards the key distribution channel from eavesdropping.

## References

[1] H. K. Lo, M. Curty, and K. Tamaki, "Secure quantum key distribution," Nature Photonics **8**, 596-604 (2014).
[2] K. Kravtsov, Z. Wang, W. Trappe, and P. R. Prucnal, "Physical layer secret key generation for fiber-optical networks," Opt. Express **21**, 23756-23771 (2013).
[3] B. Wu, Z. Wang, Y. Tian, M. P. Fok, B. J. Shastri, D. R. Kanoff, and P. R. Prucnal, "Optical steganography based on amplified spontaneous emission noise," Opt. Express **21**, 2065-2071 (2013).
[4] 100G CI-BCH-4 eFEC technology (www.microsemi.com).
[5] G. Brassard, et al, "Secret-key reconciliation by public discussion," in Workshop on the theory and application of cryptographic techniques on Advances in cryptology, (EUROCRYPT, Secaucus, NJ, USA, 1994), pp. 410–423.