Analog noise protected optical encryption with two-dimensional key space

Ben Wu,* Matthew P. Chang, Bhavin J. Shastri, Zhenxing Wang, and Paul R. Prucnal

Lightwave Communications Laboratory, Department of Electrical Engineering, Princeton University, Princeton, NJ 08544, USA

benwu@princeton.edu

Abstract: An optical encryption method based on analog noise is proposed and experimentally demonstrated. The transmitted data is encrypted with wideband analog noise. Without decrypting the data instantly at the receiver, the data is damaged by the noise and cannot be recovered by post-processing techniques. A matching condition in both phase and amplitude of the noise needs to be satisfied between the transmitter and the receiver to cancel the noise. The precise requirement of the phase and amplitude matching condition provides a large two-dimensional key space, which can be deployed in the encryption and decryption process at the transmitter and receiver.

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

References and links

1. B. Wu, B. J. Shastri, and P. R. Prucnal, "Secure communication in fiber-optic networks," in *Emerging Trends in ICT Security*, B. Akhgar and H. Arabnia, eds. (Elsevier, 2014).
2. 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**(2), 2065–2071 (2013).
3. M. P. Fok, Z. Wang, Y. Deng, and P. R. Prucnal, "Optical layer security in fiber-optic network," IEEE Trans. Inf. Forensics Security **6**(3), 725–736 (2011).
4. B. Wu, Z. Wang, B. J. Shastri, M. P. Chang, N. A. Frost, and P. R. Prucnal, "Temporal phase mask encrypted optical steganography carried by amplified spontaneous emission noise," Opt. Express **22**(1), 954–961 (2014).
5. G. D. VanWiggeren and R. Roy, "Communication with chaotic lasers," Science **279**(5354), 1198–1200 (1998).
6. A. Argyris, D. Syvridis, L. Larger, V. Annovazzi-Lodi, P. Colet, I. Fischer, J. García-Ojalvo, C. R. Mirasso, L. Pesquera, and K. A. Shore, "Chaos-based communications at high bit rates using commercial fibre-optic links," Nature **438**(7066), 343–346 (2005).
7. P. Li, J. G. Wu, Z. M. Wu, X. D. Lin, D. Deng, Y. R. Liu, and G. Q. Xia, "Bidirectional chaos communication between two outer semiconductor lasers coupled mutually with a central semiconductor laser," Opt. Express **19**(24), 23921–23931 (2011).
8. H. Soto, D. Erasme, and G. Guekos, "5-Gb/s XOR optical gate based on cross-polarization modulation in semiconductor optical amplifiers," IEEE Photon. Technol. Lett. **13**(4), 335–337 (2001).
9. J. H. Kim, Y. M. Jhon, Y. T. Byun, S. Lee, D. H. Woo, and S. H. Kim, "All optical XOR gate using semiconductor optical amplifiers without additional input beam," IEEE Photon. Technol. Lett. **14**(10), 1436–1438 (2002).
10. T. Fjelde, D. Wolfson, A. Kloch, B. Dagens, A. Coquelin, I. Guillemot, F. Gaborit, F. Poingt, and M. Renaud, "Demonstration of 20 Gbit/s alloptical logic XOR in integrated SOA-based interferometric wavelength converter," Electron. Lett. **36**(22), 1863–1864 (2000).
11. K. Chan, C. K. Chan, L. K. Chen, and F. Tong, "Demonstration of 20-Gb/s all-optical XOR gate by four-wave mixing in semiconductor optical amplifier with RZ-DPSK modulated inputs," IEEE Photon. Technol. Lett. **16**(3), 897–899 (2004).
12. J. Suarez and P. R. Prucnal, "Instantaneous bandwidth of counter-phase optical interference cancellation for RF communications," IEEE Microwave Wireless Components **21**(9), 507–509 (2011).
13. J. Suarez, K. Kravtsov, and P. R. Prucnal, "Methods of feedback control for adaptive counter-phase optical interference cancellation," IEEE Trans. Instrum. Meas. **60**(2), 598–607 (2011).
14. M. P. Chang, M. Fok, A. Hofmaier, and P. R. Prucnal, "Optical analog self-interference cancellation using electro-absorption modulators," IEEE Microwave Wireless Components **23**(2), 99–101 (2013).
15. J. Chang and P. R. Prucnal, "A novel analog photonic method for broadband multipath interference cancellation," IEEE Microwave Wireless Components **23**(7), 377–379 (2013).
16. B. Wu, M. P. Chang, Z. Wang, B. J. Shastri, and P. R. Prucnal, "Optical encryption based on cancellation of analog noise," in *Proceedings of CLEO* (Optical Society of America, 2014), paper AW3P.5 (to be published).

#210801 - $15.00 USD Received 24 Apr 2014; revised 29 May 2014; accepted 30 May 2014; published 5 Jun 2014

1. Introduction

With the increasing usage of optical networks and the requirement of bandwidth, it is important that the transmitted data is properly secured without compromising the data rate [1,2]. Optical encryption can protect the confidentiality and privacy of data transmission with low latency and high speed [3,4]. Different ways to achieve optical encryption have been studied. Optical chaotic encryption uses a feedback loop to generate a wideband chaotic noise [5–7]. This spread spectrum technique both protects the confidentiality of the signal and avoids the malicious jamming to the data channel. Optical XOR logic encryption provides another way of high-speed encryption. Several different approaches have been studied to realize optical XOR functions [8–11] and the data rate of the encryption process reaches 20Gb/s [10,11]. Although optical XOR logic can encrypt the data with high speed, the encrypted data is a still a digital signal. Compared with signals encrypted with analog noise, which cannot be digitized by the receiver without decryption, the encrypted digital signal carries all the information of the original signal. Even without knowing the key for the encryption process, an eavesdropper can record the encrypted digital signal and use post-processing technique to recover the original data. Optical chaotic encryption encrypts the data with noise-like analog signals and the transmitted data cannot be recovered if the receiver cannot decrypt the data instantly. The decryption process requires the chaotic systems at the transmitter and the receiver to be synchronized [5]. The requirement of synchronization parameters between chaotic systems cannot be directly used as the key for the encryption process and the key space for different parameters has not been well studied. Considering both the case of optical XOR logic and optical chaotic encryption, an encryption method with noise like encrypted signal and easily controllable parameters for large key space is required.

Optical interference cancellation techniques can be used as an encryption method that satisfies the requirement of high speed, noise like encrypted signals and large key space. Optical interference cancellation has been applied to remove interference in wireless communication networks [12–15]. To effectively cancel the interference noise, the most challenging problem is to satisfy the matching condition between the interference signal and the cancellation signal. Because the interference noise has wide bandwidth, which overlaps with the signal of interest, the cancellation process requires precisely matching the optical delay and amplitude between the interference path and cancellation path of the noise. While the fine requirement of the matching condition is a challenging problem for optical interference cancellation, it can actually be an advantage for the optical encryption. The precise requirement of optical delay and attenuation provides a large key space to the encryption process. Without knowing both the phase and amplitude of the noise, the eavesdropper cannot recover the encrypted signals.

In this paper, an optical encryption system based on interference noise cancellation is designed and experimentally demonstrated. The transmitted digital signal is encrypted with analog noise with wide bandwidth and amplitude stronger than the digital signal. The encrypted signal is noise-like and cannot be digitized by the receiver, so an eavesdropper cannot be recover the signal by post-processing technique. Moreover, the decryption process requires matching both the optical delay and optical attenuation between the transmitter and receiver. Both optical delay and optical attenuation can be used as key for the encryption process and forms a large two-dimensional key space.

2. Experiment setup

The encryption system includes two channels with different wavelengths λ_1 = 1550.12nm and λ_2 = 1551.72 (Fig. 1). Both of the lasers at the transmitter have a output power of 10dBm. The signal with interference noise is carried by channel 1(C_1) and the cancellation noise is carried by channel 2(C_2).

$$C_1 = S_1 + N_1. \tag{1}$$

$$C_2 = N_2. \tag{2}$$

#210801 - $15.00 USD Received 24 Apr 2014; revised 29 May 2014; accepted 30 May 2014; published 5 Jun 2014

where S_1 is the transmitted signal and N_1 is the interference noise in channel 1. N_2 is the cancellation noise in channel 2. The signal used in the experiment is pseudorandom binary sequence (PRBS) with length 2^{31}-1. The interference noise and the cancellation noise are radio frequency (RF) noise and come from the same source (Fig. 1). The interference noise N_1 has a strong amplitude and bandwidth overlap with the signal to protect the signal from being decrypted. Both of the channels are sent over 25km standard single mode fiber (SSMF) with dispersion compensation (Fig. 1). At the receiver, a WDM filter with 3dB bandwidth 0.5nm is used to split the two channels and then the two channels are amplified separately by two EDFAs with 16dB gain. The two channels are feed into the positive and the negative inputs of a balanced photo detector. The balanced photo detector subtracts the cancellation noise in channel 2 from the interference noise from channel 1 and recovers the signal. To effectively remove the noise, the interference noise and cancellation noise has to match in both the phase and the amplitude. The phase is controlled by a pair of tunable optical delays at the transmitter and the receiver and the amplitude is controlled by an pair of tunable optical attenuators (Fig. 1). Both of the phase and amplitude can be changed dynamically. The requirement of phase and amplitude matching are orthogonal to each other, which forms a two-dimensional key space. The attenuator at the transmitter is added before the modulator, so the amplitude of RF noise and the power of the optical carrier can be adjusted separately and both of them determine the amplitude of the encryption noise.

In the experiment, the data rate of the signal is 10Gb/s. A sine wave with its frequency changing between 4GHz to 7GHz is used as the noise. The noise deployed in the system overlaps with the zero-order lobe of the signal spectrum. If the eavesdropper uses a band pass filter to remove the noise, the signal in this frequency range is also removed and cannot be recovered. The optical path difference between the two channels at the transmitter is designed to be 10m. The experimental results in section 3 show that the optical delay has to be matched within 1mm, which means without knowing of the optical delay, the eavesdropper needs to find the correct 1mm length in the range of 10m in order to decrypt the data. Moreover, to match the optical delay does not indicate the matching condition of the amplitude. The requirement of the amplitude matching increases the key space geometrically. To stabilize the matching condition, temperature control is provided at the transmitter and receiver. A heating system with temperature sensing and feed back control to is used to control the temperature.

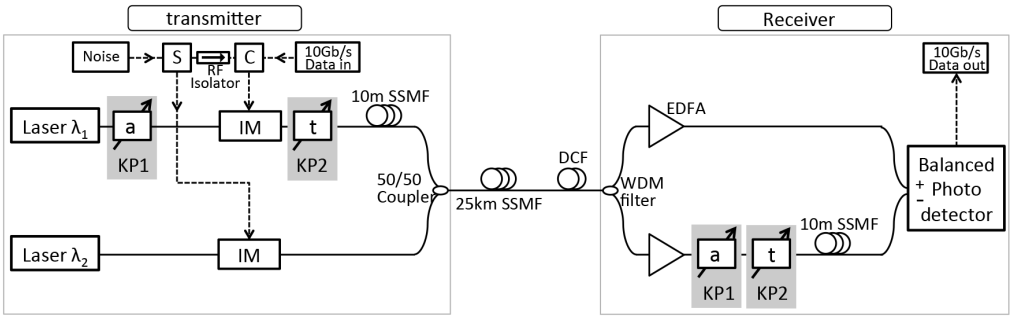

Fig. 1. Experimental Setup, the dash line shows the electric signal and the solid shows the optical signal (RF: Radio frequency; S: RF splitter; C: RF combiner; KP: key pair; a: tunable attenuator; t: tunable time delay; IM: intensity modulator; SSMF: standard single mode fiber; DCF: dispersion compensation fiber; EDFA: erbium-doped fiber amplifier; WDM: wavelength division multiplexer).

3. Experiment results and analysis

3.1 BER measurement in two-dimensional key space

The eye diagram measurement shows that a clear eye diagram can only be received when both phase and amplitude of the noise in the two paths are matched (Fig. 2). The clear eye diagram in Fig. 2(a) corresponds to a minimum of BER in a two-dimensional key space (Fig. 3). When

#210801 - $15.00 USD Received 24 Apr 2014; revised 29 May 2014; accepted 30 May 2014; published 5 Jun 2014

the cancellation noise is not applied, the signal is completely noisy because of the analog interference (Fig. 2(b)). The eye diagram has no opening and the receiver cannot digitize the signal. When cancellation noise is applied with either phase mismatch (Figs. 2(c) and 2(d)) or amplitude mismatch (Figs. 2(e) and 2(f)), the eye diagram is still noisy, which leads to a large BER. Figure 2(c) is the eye diagram when the phase is not matched and corresponds to point A in the BER measurement of Fig. 3(a). Figure 2(e) is the eye diagram when the amplitude is not matched and corresponds to point B in the BER measurement of Fig. 3(b). Figures 2(d) and 2(f) show that when the phase and amplitude mismatch increase further, the eye diagram becomes noisier.

The BER measurement shows that the BER increases exponentially when either phase or amplitude is not matched. A minimum BER of 7×10^{-4} is achieved when the matching condition is satisfied (Fig. 3). Forward error correction (FEC) with Reed-Solomon code can be used to reduce a BER of 7×10^{-4} to where it is error free [16]. The optical delay range that leads to BER lower than the FEC limit is less than 1mm (Fig. 3(a)) and the optical path difference between the two channels at the transmitter is designed to be in the order of 10m. Without pre-known information about the optical delay, an eavesdropper has to find 1mm in the 10m range in order decrypt the data. The case is similar for the amplitude matching. The amplitude range that leads to BER lower than the FEC limit is less than 0.53dB. As the optical delay and the amplitude can be changed independently, matching one of them does not indicate any information about the other; these two parameters are orthogonal and form a two-dimensional key space (Fig. 3(c)).

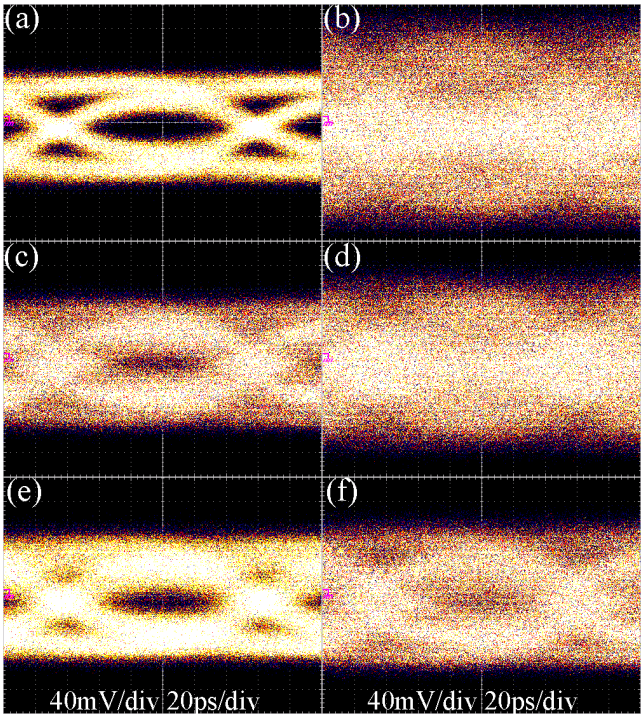

Fig. 2. Eye diagram in different conditions: (a) Both optical delay and amplitude are matched. (b) Signal and interference noise without cancellation. (c) Optical delay is not matched with 1.8mm mismatch. (d) Optical delay is not matched with 3.6mm mismatch. (e) Amplitude is not matched with 1.4dB mismatch. (f) Amplitude is not matched with 2.8dB mismatch.

#210801 - $15.00 USD Received 24 Apr 2014; revised 29 May 2014; accepted 30 May 2014; published 5 Jun 2014

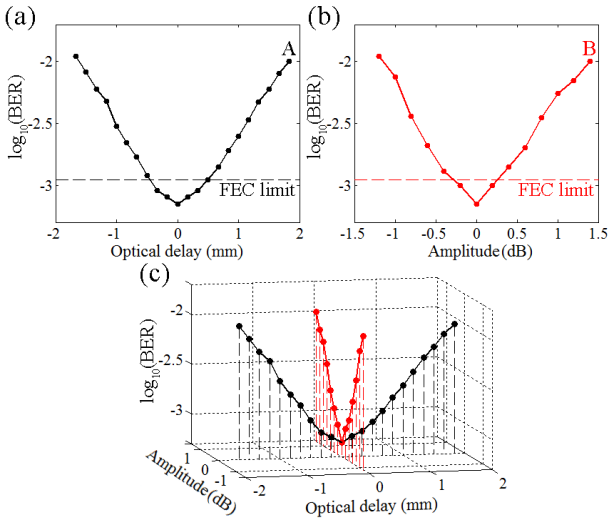

Fig. 3. (a) BER measurement as the optical delay changes. (b) BER measurement as the cancellation noise amplitude changes. (c) BER in a two dimensional view.

3.2 Frequency response

The RF transmission spectrum shows that an average noise cancellation of 26dB can be achieved within the bandwidth of 4GHz to 7GHz when both the phase and amplitude is matched (Fig. 4). In this experiment, a network analyzer is used to measure the frequency response of the system. An RF signal scanning from 4GHz to 7GHz is used as the noise input for both of the channels. The RF transmission spectrum (S_{21}) is measured at the receiver. In Fig. 4, the cancellation spectrum is the frequency response of the transmitter and receiver when the matching condition between the two channels is satisfied. The reference spectrum is the frequency response of a single channel. By subtracting the cancellation spectrum by the reference spectrum, an average cancellation of 26dB is achieved within the bandwidth of 4GHz to 7GHz. The ripple of the cancellation spectrum results from the reflection in the RF components and frequency mismatch between the two channels.

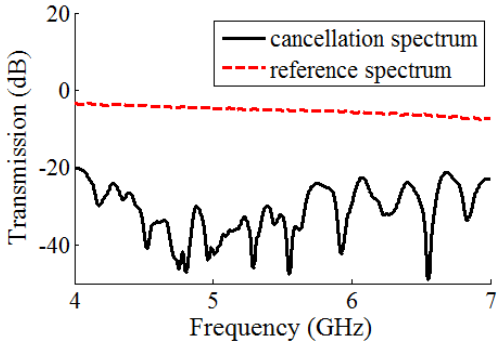

Fig. 4. The transmission spectrum of the encryption system.

Simulation results show that the noise bandwidth of 4-7GHz is wide enough to encrypt and protect a signal with the data rate of 10Gb/s. If an eavesdropper cannot find the matching condition and tries to use a perfect RF filter to remove the noise between 4GHz and 7GHz (Figs. 5(a) and 5(b)), the signal information in this frequency range also lost. The loss of information in the frequency domain leads to a closed eye diagram (Figs. 5(c) and 5(d)). The comparison of the clear eye diagram with the zero-order lobe of the spectrum unchanged (Fig. 5(c)) and noisy eye diagram with the frequency range of 4-7GHz removed (Fig. 5(d)) shows

#210801 - $15.00 USD Received 24 Apr 2014; revised 29 May 2014; accepted 30 May 2014; published 5 Jun 2014

that this frequency range is wide enough and is indispensable for the signal. In the simulation, a PRBS with length 2^{15}-1 is used as the signal. The simulation only considers the effect of spectrum component loss. In the communication system, the system noise will degrade the eye diagram in Fig. 5(d) even further.

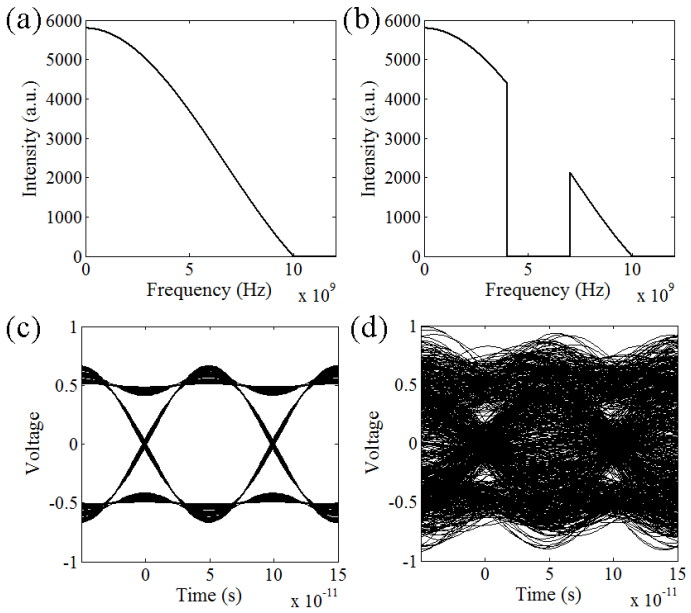

Fig. 5. (a) RF spectrum of the 10Gb/s data (b) RF spectrum of 10Gb/s data with 4-7GHz frequency range removed (c) Eye diagram of the 10Gb/s data (d) Eye diagram of the 10Gb/s data with 4-7GHz frequency range removed.

3.3 Secure analysis

An eavesdropper cannot measure the amplitude difference of the noise between channel 1 and channel 2. The noise and signal in channel 1 are always combined and noisy like (Fig. 2(b)). Without separating the noise and signal in channel 1, the amplitude of the noise in channel 1 cannot be measured.

The BER measurement results in Fig. 3 show that a minimum of BER is achieved when the matching condition is satisfied. An eavesdropper without knowing either the transmitted signal or the clock of the signal cannot measure the BER and has to receive the noisy time domain signal (Fig. 2(b)). Even the eavesdropper uses a scanning technique and finds some changing trend of the noise amplitude, both of the amplitude and delay can change rapidly and the eavesdropper cannot find the matching condition before it changes. To ensure the transmitter and the receiver share the same key sequence, key distribution is needed. The key distribution can be accomplished by the optical steganography method, where the key is transmitted separately in a stealth channel [2,4].

The optical delay length used in the experiment is 10m, which can be increased further to enlarge the key space. If the phase of the noise is completely random, there is no limit on the optical delay length difference. The measured 1mm delay matching range and 0.53dB amplitude matching range are optimized values to have the BER at the matching point just below the FEC limit. The matching range depends on the receiver noise, the forward error correction limit and the amplitude ratio between the encryption noise and the signal.

3.4 System analysis

The encryption method can be applied to a WDM system. Each WDM channel carries signal and analog noise. All the WDM channels share an additional channel, which carries only

#210801 - $15.00 USD Received 24 Apr 2014; revised 29 May 2014; accepted 30 May 2014; published 5 Jun 2014

noise. The analog noise of all the WDM channels comes from the same source but have different amplitudes and delays. To decrypt the signal, each WDM channel needs to adjust the phase and the amplitude of the noise in the shared channel to match and cancel the noise in their own channel.

The RF noise in this encryption method is carried by the optical channel with standard intensity modulation. The experiment use 25km fiber to demonstrate the transmission of the encrypted signal. The encrypted signal can be transmitted through the existing public network with longer distance. This encryption method does not require the optical carrier to reach high power level and nonlinear effect is not observed in the experiment.

4. Conclusion

We have proposed and experimentally demonstrated an optical encryption method based on the cancellation of analog RF noise. The wide bandwidth and analog properties of the noise enable the encrypted signal to be noise-like so the eavesdropper cannot digitize the encrypted signal. The decryption process requires precisely matching both the phase and amplitude of the noise, which provide a two-dimensional key space. The experiment results show that to match the phase, an eavesdropper need to find 1mm optical delay in a 10m range in order to decrypted the data. The amplitude matching require to matching the amplitude within 0.53dB. The bandwidth of the noise range from 4GHz to 7GHz and without effectively cancel the noise, it will always overlap with the signal spectrum and damage the transmitted signal.

Acknowledgments

The authors would like to thank Yue Tian and John Chang in the Lightwave Communications Laboratory at Princeton University for help with lab and equipment maintenance.

#210801 - $15.00 USD Received 24 Apr 2014; revised 29 May 2014; accepted 30 May 2014; published 5 Jun 2014