Optical Signal Processing and Stealth Transmission for Privacy

Ben Wu, Bhavin J. Shastri, *Member, IEEE*, Prateek Mittal, *Member, IEEE*, Alexander N. Tait, *Student Member, IEEE*, and Paul R. Prucnal, *Fellow, IEEE*

***Abstract*—Optical encryption, key generation, and optical stealth transmission techniques for protecting the privacy of communication in optical networks are proposed and summarized. The signal processing methods based on fiber components provide ways to encrypt data and generate encryption keys at the speed of data transmission in optical fibers. Private and confidential communication is achieved without compromising the capacity and bandwidth of the optical network. Optical stealth transmission can hide the signal in plain sight. Because an eavesdropper can neither read the data nor detect the existence of the transmitted signal, optical stealth transmission provides a higher level of privacy. A hybrid system which includes both the public channels and stealth channels can effectively provide anonymous communication and defend against traffic analysis.**

***Index Terms*—Optical encryption, key distribution, photonic neurons, optical steganography, amplified spontaneous emission, interference cancellation.**

I. Introduction

THE remarkable proliferation of broadband information technology requires that data be transmitted at high speeds and long distances over fiber optic networks. As with other communication media, fiber optics are subject to security and privacy threats, especially when the network spans large geographic domains encompassing different national interests. Even within the jurisdiction of a single country, treats from both internal and external security attacks are ever-present. Therefore, providing both confidentiality and privacy in today's fiber optic networks is a critical need.

Although confidentiality and privacy can be supported through conventional higher-layer services, these security objectives may be better supported in the physical or "optical layer" by using the unique and ultra-fast properties of optical signal processing [1], [2]. In particular, confidentiality can be supported by optically processing and encrypting the data in real time without generating an electromagnetic signature [1]. Similarly, privacy can be supported by using optical techniques to mask the existence of communications in the optical network, or by stealthily hiding optical signals using the natural physical characteristics of the optical channel.

Different approaches to optical signal processing with fiber-based techniques have been studied by the optics community. These approaches include optical XOR logic encryption [3]–[9], optical code division multiplexing (Optical CDMA) [10]–[16] and optical chaotic encryption [17]–[23]. Optical XOR logic can reach a real-time 20 Gb/s encryption speed. Optical CDMA techniques not only protect the transmitted data but also provide a multiplexing method that enables multiuser sharing of the optical network. Optical chaotic encryption encrypts the transmitted data as noise-like signals, so the eavesdropper cannot digitize the encrypted signal. Without decrypting the data when receiving the optical signal, the eavesdropper is unable to recover the data.

Previously proposed optical signal processing techniques can effectively protect the security and privacy of the data; however, they still have several disadvantages. For example, optical XOR logic encrypts the transmitted data with another data sequence by performing XOR logic of the two data sequences. Because the encrypted data signals remains in digital form [3]–[9], even if the eavesdropper cannot find the correct key, the data can be recorded and recovered using post-processing decryption. Chaos encryption effectively solves this problem, but it requires synchronization between the transmitter and receiver, and the synchronization parameters cannot be directly used as the key for the encryption process [17], [18]. Therefore, a technique having both analog noise encryption as well as parameters that can be used for the encryption key is required.

It is not only desirable to use analog noise-based optical encryption with a suitable key, but it is also necessary to generate and distribute the key. The security level of the system depends strongly on the length of the key and how frequently the key can be changed. Quantum key distribution has been widely studied for this purpose [24], [25], though the stability of quantum key distribution has not yet been demonstrated for practical applications.

In addition to encryption, an alternative for protecting the privacy of the optical network is stealth transmission. Encryption can prevent the data being read by an eavesdropper, while the existence of the signal is still exposed. In some cases, even the exposure of the encrypted data can enable a malicious attack on the system. To hide the existence of the signal, stealth transmission is needed.

Several optical signal processing techniques for privacy are presented in this review paper, including an optical encryption

Manuscript received October 21, 2014; revised March 16, 2015; accepted March 27, 2015. Date of publication April 20, 2015; date of current version September 14, 2015. The guest editor coordinating the review of this manuscript and approving it for publication was Prof. Wade Trappe.

The authors are with the Department of Electrical Engineering, Princeton University, Princeton, NJ 08544 USA (e-mail: benwu@princeton.edu; bshastri@princeton.edu; pmittal@princeton.edu; atait@princeton.edu; prucnal@princeton.edu).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/JSTSP.2015.2424690

technique that protects the transmitted signal with analog noise, a key generation technique based on neuromorphic spike processing, and optical stealth transmission methods that can hide the existence of signals. Both the optical encryption and key generation techniques utilize all-optical signal processing, as discussed in Section II. The principles of optical stealth transmission are introduced in part A of Section III, and the use of optical stealth transmission to defend against traffic analysis is discussed in part B of Section III.

II. Optical Signal Processing

A. Analog Noise Protected Optical Encryption

Interference is undesirable when transmitting and receiving data. However, if the interference can be controlled, its noise-like signature can be used to effectively carry out encryption. In this section, we will introduce a technique for control and cancellation of interference and then discuss how it can be applied to optical encryption.

Interference cancellation techniques are especially important for wireless communication [26]–[28]. If a wireless router transmits and receives signals at the same time, the transmitting antenna generates unwanted interference for the receiving antenna. Because the transmitting antenna is much closer than the source of the signal of interest, the amplitude of interference is usually much larger than the amplitude of the signal. We have previously developed a technique to cancel the interference in which the transmitting antenna is connected internally though a fiber link with the receiving antenna. This is illustrated in Fig. 1, where the fiber link is shown within the dashed rectangle. The fiber link includes two channels with two lasers and converts the electric signals from both the transmitting antenna and receiving antenna into optical signals by intensity modulation [26]. The signal from the receiving antenna contains both the signal of interest and the interference, while the signal from the transmitting antenna only contains interference. The fiber link can invert the signal from the transmitting antenna using optical devices and sum the signals from the two antennas. Since the signal from the transmitting antenna is inverted, it can cancel the interference from the receiving antenna.

The benefit of using the fiber link for interference cancellation is not only that it achieves high speed and real-time processing, but also that it reaches a high cancellation ratio of 30 dB [26]. The challenge for this method is that the phases and amplitudes of the interference in the two channels have to be precisely matched in order to be canceled by each other [26]. If either phase or amplitude is not matched, the cancellation ratio will decrease significantly with the mismatch.

Both the benefit and challenge of this cancellation technique are actually benefits if this technique is applied as an encryption method [29], [30]. The interference noise can serve as analog noise accompanying the transmitted signal. The precise requirement of amplitude and phase matching can be used as the key for the encryption process [29]. The high-speed property of the fiber optic processing method satisfies the requirement of large bandwidth and real time processing of the signal encryption. In our experiment, we have achieved 10 Gb/s encrypted data transmission with real time encryption in a 25 km fiber link

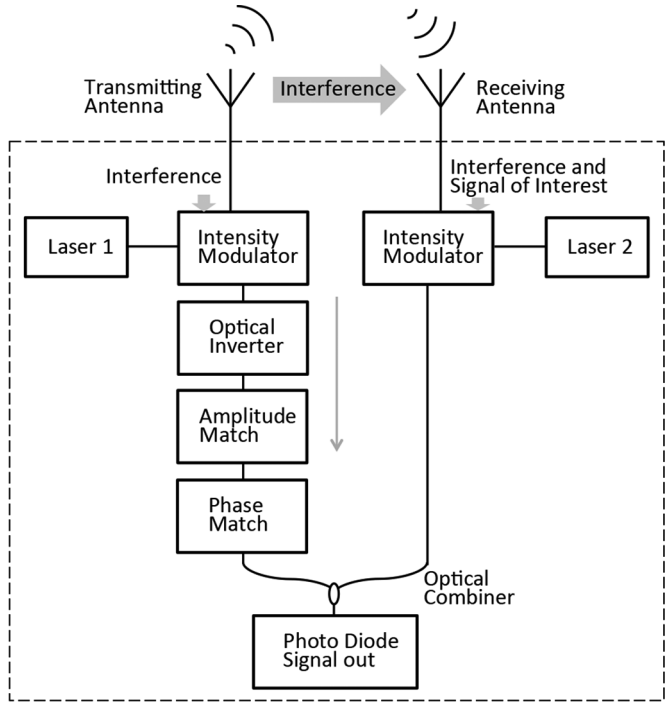


Fig. 1. Schematic diagram of interference cancellation.

[29]. The signal is disguised as natural analog noise, and only by matching both the amplitude and phase of the analog noise between transmitter and receiver can the receiver decrypt the signal. The analog noise shares the same frequency range with the signal, so that the noise cannot be removed by filters. If the eavesdropper cannot find the matching condition, the signal cannot be digitized. If the signal cannot be decrypted when being received, the data is lost and cannot be recovered by a post-processing technique.

The schematic diagram of the encryption system reveals that the transmitter is very similar to the interference cancellation system (Fig. 2). The only difference is that, in the interference cancellation system, the amplitude and phase are designed to be matched, while in the transmitter of the encryption system, the amplitude and phase differences are generated deliberately, so both of the parameters can be used as keys for encryption. The signals in Channel 1 (C_1) and Channel 2 (C_2) can be described as:

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

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

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 [29]. To decrypt the signal, the amplitude and phase of N_1 and N_2 have to be matched at the receiver. Fig. 3 shows the measured eye diagrams of the encrypted signal [29]. When the interference is cancelled by the receiver, a clear eye diagram is received (Fig. 3(a)); when the interference is not cancelled, the signal is noisy and cannot be digitized (Fig. 3(b)).

This technique is also suitable for multi-user wavelength division multiplexing (WDM) systems. For a single user, the encryption system needs two channels with different wavelengths.

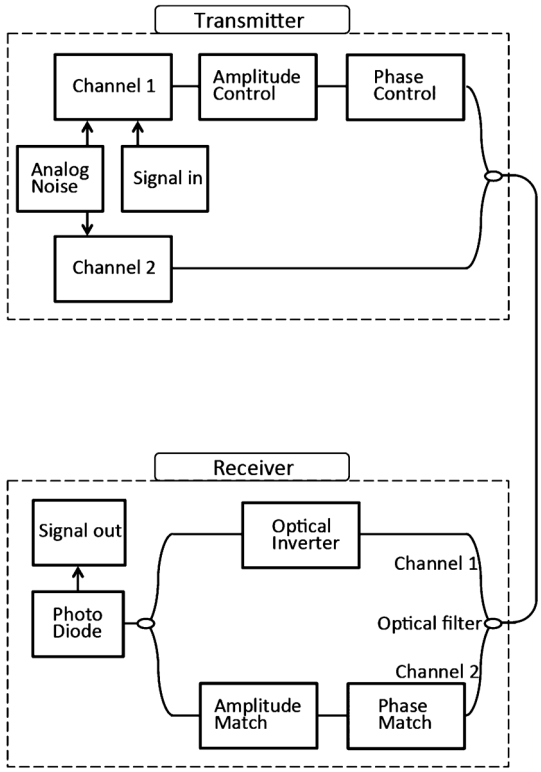


Fig. 2. Schematic diagram of analog noise encryption system.

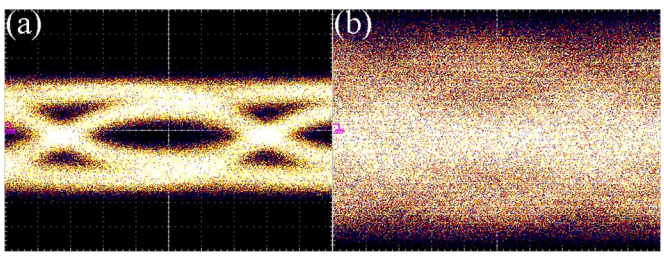


Fig. 3. (a) Eye diagrams of the encrypted signals with the interference cancelled (b) Eye diagrams of the encrypted signals without the interference cancelled. This figure is from [29].

In the case of a multi-user WDM system, the different users deploying multiple WDM channels can share the same channel for carrying the analog noise used for cancellation (Fig. 4). Different WDM channels can use different keys for the encryption, which means different amplitude and phase of the interference noise signal is applied.

The number of channels that share one cancellation channel is limited by the signal-to-noise ratio (SNR) of the cancellation channel, because the power of the cancellation channel is decreased by splitting into multiple users. The decreased power can be compensated by optical amplifiers; however, the SNR of the cancellation signal degrades after being amplified so that the interference in the signal cannot be effectively cancelled. Here we provide a simple model to calculate how many channels are supported. In this model, the input optical power of the cancellation channel is 1 mW and it has 5 dB loss after 25 km transmission. A receiver splits and receives part of the cancellation signal and then uses an EDFA to amplify the signal. To calculate the SNR of the cancellation signal after it is amplified

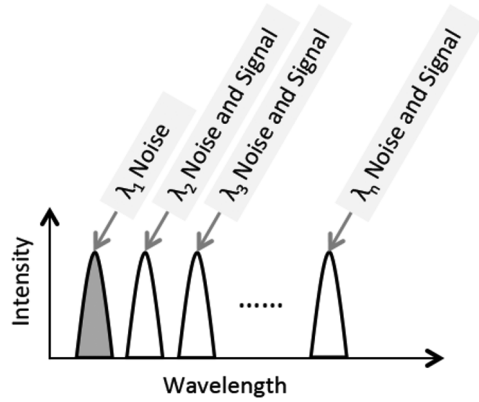


Fig. 4. Analog noise encryption in a wavelength division multiplexing (WDM) system.

by the EDFA, we assume that the noise is dominated by the beat noise between the signal and the ASE generated by the EDFA. In this case, the SNR can be calculated as [31]:

$$SNR = \frac{GP_{in}}{4S_{sp}\Delta f} \tag{3}$$

Where G is the gain the EDFA, P_{in} is the optical input power of the EDFA, Δf is the bandwidth of the receiver (which is 10 GHz in our experiment), and S_{sp} is the spectral density of the ASE noise from EDFA. S_{sp} can be written as:

$$S_{sp} = (G-1)n_{sp}hv \tag{4}$$

where n_{sp} is the population-inversion factor (which is close to 1 for an ideal amplifier) [31] and $h\nu$ is the photon energy. Substituting (4) into (3) and assume $\mathrm{G} \gg 1$, we get:

$$SNR = \frac{P_{in}}{4hv\Delta f} \tag{5}$$

The criterion for judging whether the SNR of the cancellation signal is adequate for decryption is that the noise cannot accumulate to a level that affects the amplitude matching between the interference signal and cancellation signal. The experimental measurement shows that the amplitude matching tolerance in terms of optical power is 0.53 dB as a full-width range, or 0.265 dB as a half width range [29]. This means the optical noise power cannot be higher than $(10^{0.0265}-1)\times 100 = 6\%$ of the optical signal power, or in other words, the SNR in (5) cannot be lower than $(100\%/6\%)^2 = 289 = 25$ dB. The square comes from the fact that the power of the electric current in a photo-diode is proportional to the square of the optical power when calculating SNR. Therefore, the input power of the EDFA in (5) can be calculated as $\mathrm{P_{in}} = 25\ \mu$W, which is the minimum input power of the EDFA at the receiver to achieve effective demodulation. Since the launched optical power of the cancellation signal is 1 mW, it is attenuated to 0.3 mW after 25 km transmission. The cancellation channel can support a maximum of 0.3 mW/25μ W $= 12$ channels. This theoretical analysis provides a direct understanding of which factors may affect the number of channels that can share a cancellation channel.

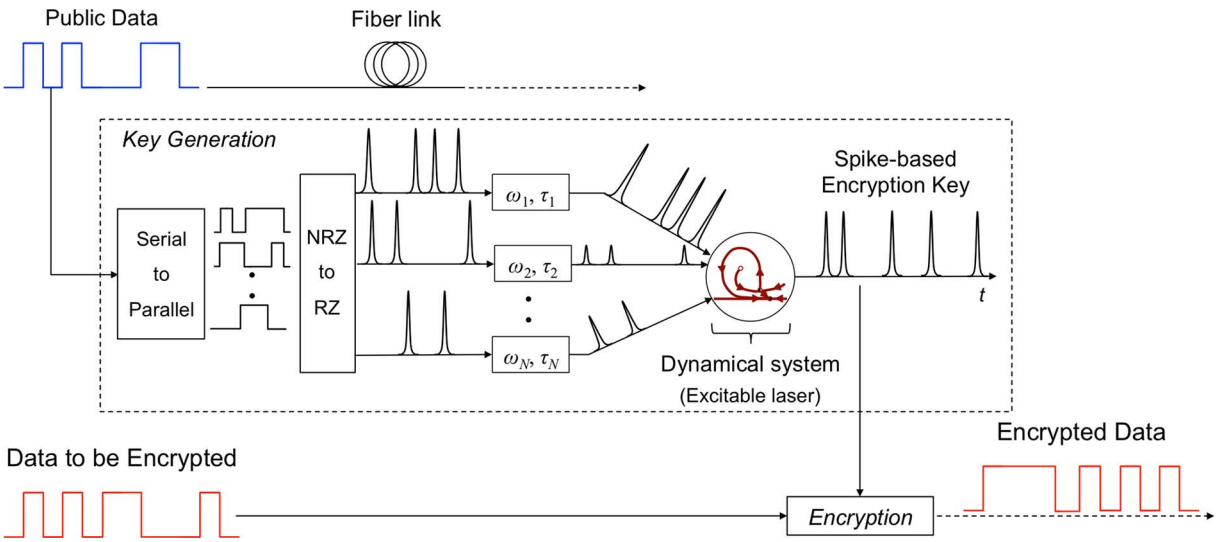


Fig. 5. Schematic diagram of key generation based on neuromorphic spike processing.

B. Key Generation Based on Neuromorphic Spike Processing

Neuromorphic spike processing—a hybrid analog and digital processing technique inspired by neuroscience—is a sparse-based coding scheme where information is encoded as events. It takes advantage of both the bandwidth efficiency of analog computation and the noise robustness of digital computation [32], making the spike-based approach attractive for information processing. Recently, there has been a significant interest in photonic bio-inspired computing [33]–[42] in which the biophysics of neural computation algorithms are exploited in the context of harnessing the high speed, high bandwidth, and low crosstalk available to photonic interconnects [40]–[43] to potentially grant the capacity for complex, ultrafast categorization and decision-making [35]. This could provide a wide range of computing and signal processing applications (e.g., adaptive control, real-time embedded system analysis, and cognitive RF processing).

Here we propose the simple idea of using photonic neuromorphic signal processing for key generation. More specifically, our scheme involves exploiting the public data to generate a dynamically changing spike-based key by employing a nonlinear dynamical excitable system. The generated key can be used for optical encryption. A system is said to be excitable if it is at an attracting equilibrium state, but can be triggered by a small perturbation to produce a large amplitude excursion, after which the system settles back to the attractor in what is called the refractory phase [44]. We recently discovered [45] a close analogy between the dynamics of lasers and those of spiking biological neurons, both of which can exhibit excitability.

In this scheme, the idea is to use the public channel to generate an encryption key that is spike-based (Fig. 5). This is done all-optically by first performing a serial to parallel conversion with a 1:N deserializer [46]. Next, the parallel non-return-to-zero (NRZ) bits are converted to their equivalent return-to-zero format (RZ) [47]. Each of these pulses is weighted and delayed to create spatiotemporal patterns before being spatially summed. The resulting pulse train is input to an excitable laser which performs temporal integration of nearby pulses with a time constant, firing a single spike when the integration state variable crosses a threshold. The resulting spike-based key is dynamically changing at the rate f_{data}/N; where f_{data} is the public date rate. This key can be used for encrypting secret data using either a temporal phase mask [48], [49] or XOR logic [3]–[9]. The data being encrypted would also need to have a bit rate of f_{data}/N. A simple phase-locked loop would be needed for phase synchronization between the spike key (used as a phase mask) and the data being encrypted. The encrypted data cannot be recovered by an eavesdropper without the a priori knowledge of the weights and delays utilized in the dynamical system at the transmitter. In this technique, the key does not need to be distributed on a secret channel. Since the key is generated by applying a nonlinear (non reversible) process using the public data, the public data itself can be used at the receiver to generate the key using a similar dynamical system to decrypt the secret data. Recent advances in photonic device fabrication has made it possible to build such excitable lasers that are very similar; furthermore, the inherent process variations can be compensated for by varying the pump currents to the lasers to obtain near identical dynamics (for a given set of input stimulation). Synchronization at the receiver is an issue, but can be addressed by using an initial training sequence consisting of the packet header for the secret data at the transmitter and receiver. Then the received training sequence can be matched to the public data in a way similar to that used for sync in a bit error rate tester receiver box.

This neuromorphic signal processing technique is aimed for generating and distributing keys for encryption. The public data used for generating keys is known to both the communicating pair and the adversary, however, the adversary does not how to generate the key from the public data. This key generation technique can work with any optical encryption method, such as optical chaotic encryption, temporal phase mask, or XOR logic. Taking optical chaotic encryption as an example, the keys for chaotic encryption technique are the parameters to synchronize the optical amplifier that generates chaos at the transmitter and receivers [17], [18]. These parameters can be generated by the neuromorphic signal processing technique.

The proposed all-optical processing scheme can potentially operate at data rates far in excess of what is capable with electronics and hence is attractive for fast encryption. In general, optical signal processing is also attractive because fiber-based devices neither generate an electromagnetic signature which can be observed from a distance nor can be jammed by external electromagnetic interference, hence posing less side-channel risk than their electrical counterparts.

III. Optical Stealth Transmission

A. Optical Steganography for Stealth Transmission

Privacy ensures individual control of what information may be received or collected and to whom the information may be disclosed [50]. Different from confidentiality, which assures that information is not readable to unauthorized individuals, privacy involves protecting contextual and personal information related to a communication and hiding the existence of the information from unauthorized users. Privacy requires a higher level of protection than confidentiality. Optical stealth transmission or in another words, optical steganography, is an effective way to protect privacy.

Optical steganography was first proposed in 2006 by Wu *et al.* [51]. The objective of optical steganography is to provide a stealth channel that is hidden in both the time domain and the frequency domain. Optical steganography is similar to multimedia watermarking techniques, where a stealth marker is embedded and hidden in the existing audio or image information. The methods to achieve this are different between optical steganography and watermarking. Watermarking techniques use a mathematical method to hide the marker in the public information, while optical steganography hides the stealth signal in the physically existing noise of the optical network [52]–[58].

There are two methods of hiding the stealth channel. The first method is to stretch the optical pulses by chromatic dispersion [52]. In this case, the stealth signals are return-to-zero intensity-modulated data. The stealth bits are carried by optical pulses from a mode locked laser (Fig. 6). The pulses have a narrow width in the time domain and wide spectral bandwidth in the frequency domain. The dispersion components stretch the pulses, so the amplitude of the pulse is low enough and merge into the noise (Figs. 7(a) and 7(b)). In the frequency domain, because the power of stealth channel is usually 15–20 dB lower than the public channel, and has much wider bandwidth, the spectrum of the stealth channel looks like the noise of the public channel (Fig. 7(c)).

The essence of the first method is to stretch the pulse and have the amplitude low enough to mimic the noise, while the second method is different: instead of mimicking the noise, this method directly uses the noise as a carrier [60], [61]. In fiber optic networks, optical amplifiers are widely used that compensate for attenuation but also introduce amplified spontaneous emission (ASE) noise. The ASE noise has randomized phase and degrades system performance by reducing its SNR. However, the property of randomized phase is actually a benefit for stealth transmission. Noise with random optical phase is

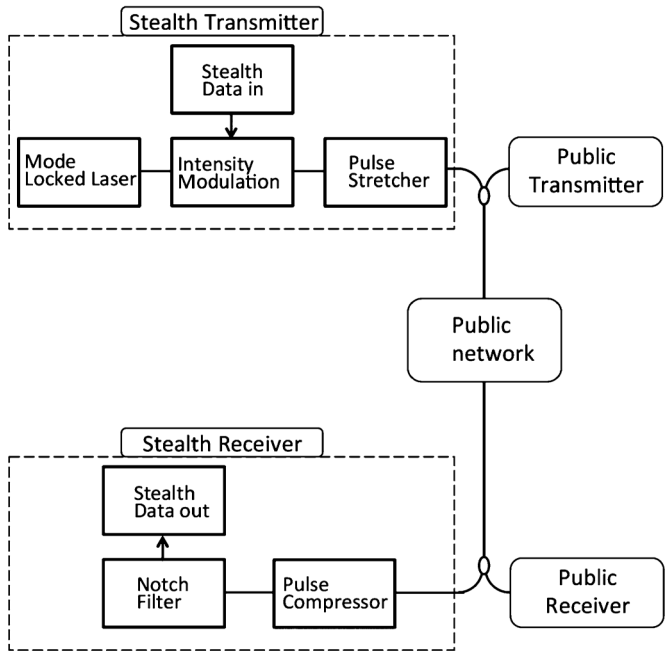


Fig. 6. Optical steganography based on pulse stretching.

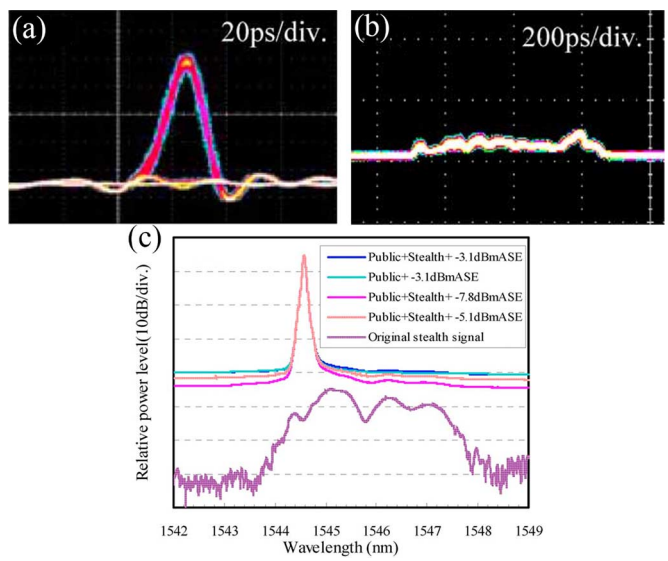


Fig. 7. (a) The stealth signal before being stretched (b) The stealth signal after being stretched (c) The spectra of the public channel and the stealth channel. This figure is from [59].

coherent only within a very short range [62]. In this scheme, the stealth transmitter and receiver form a fiber interferometer (Fig. 8) and the stealth signal is carried by phase-modulated ASE noise. If the optical delay does not match between the transmitter and receiver, constructive interference will not occur, and only ASE noise is received. Only by precisely matching the optical delay can the stealth signal, carried by ASE, interfere with itself and demodulate the data. Therefore, the random phase property of ASE noise effectively hides the signal in the time domain (Figs. 9(a) and (b)). In the frequency domain, the ASE noise covers the entire optical communication band, and the stealth channel carried by ASE has exactly the same spectrum as the original ASE (Fig. 9(c)). Therefore, the stealth channel is also undetectable in the frequency domain.

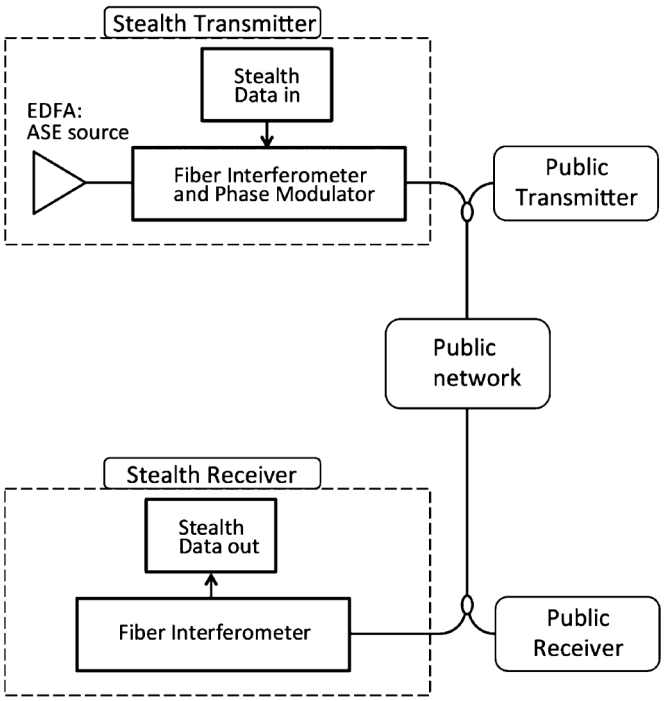


Fig. 8. Optical steganography based on ASE noise (EDFA: erbium doped fiber amplifier; ASE: amplified spontaneous emission).

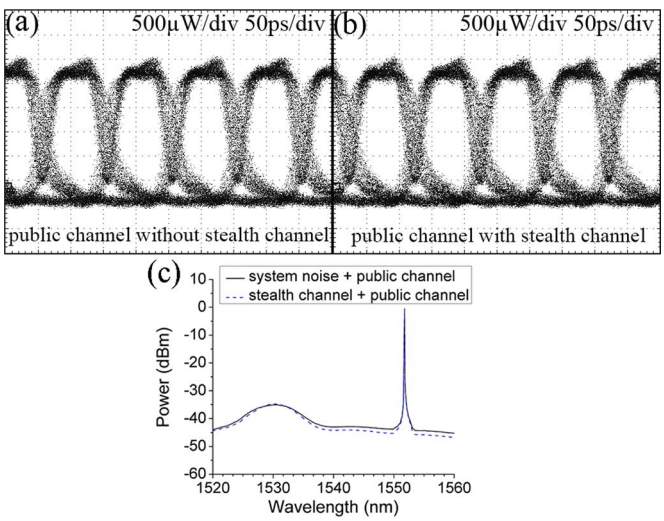


Fig. 9. (a) Eye diagram of public channel without stealth channel (b) Eye diagram of public channel with stealth channel (c) Spectrum of public channel with and without stealth channel. This figure is from [60].

ASE-based steganography uses spontaneous emission to transmit signals, which is fundamentally different from traditional fiber channels. Traditional fiber channels are carried by lasers and the SNR can be increased by increasing the power of the laser [63]. In the case of signals carried by ASE noise, the SNR saturates at a constant when optical beat noise dominates, since both the signal and the beat noise come from the ASE [64]. The constant does not depend on the power of the stealth channel and only depends on the ratio of the optical spectrum bandwidth to the electric bandwidth of the stealth channel, which is also the capacity of the stealth channel [64]–[67]. As a result, the capacity of the stealth channel is limited by the need to maintain the SNR and bit error rate below the forward error correction (FEC) limit.

To enable higher capacity of the stealth channel, wavelength-division multiplexing for the stealth channel has been studied [62]. Instead of the using the entire spectrum of the ASE noise to carry one channel, a band pass filter is used to carry the stealth signal on a portion of the ASE spectrum. The bandwidth of each stealth channel is 1.1 nm and multiple stealth channels can exist in parallel. Another benefit of having the filtered ASE spectrum as the signal carrier is that it adds another layer of security to the system. Before finding the right coherence length, the eavesdropper also needs to find the right spectral range that carries the stealth channel.

Another limitation for ASE-based optical steganography is the speed of changing the key at the transmitter. An optical delay-line can be employed as the key for hiding the stealth channel. Since the eavesdropper may use a scanning technique and find the matching condition; the optical delay length needs to be changed with time. The security level of the system is affected by the rate of change. Optical delays controlled by mechanical devices have dynamic time constants on the order of seconds. To provide a faster changing scheme, a temporal phase mask is applied [48], [49]. The phase mask is implemented with a phase modulator, which can be changed in every stealth bit. The rate of change can be in the order of nanoseconds, nine orders of magnitude faster the changing a mechanical optical delay.

Besides changing the key rapidly, the size of the key space also impacts the security level of a system. Both a phase mask and an optical delay can be used as the key for the stealth channel. The number of available phase mask codes depends on the ratio between the bandwidth of phase mask to the bandwidth of the stealth channel. The ratio is limited by the noise properties of the ASE. In the experiment, the ratio is 16 and the code space is 18,000 [48]. The key space of the optical delays does not have a limit. Because the phase of the ASE noise is completely random, there is no limit on the delay length difference. Besides phase masks and optical delays, dispersion can also be used as the key for hiding the stealth channel [68]. The dispersion can be generated by dispersion compensation fiber, photonic crystal fiber, or chirped fiber Bragg gratings [69], [70]. Since both dispersion and optical delay have to be matched between the transmitter and receiver, they are orthogonal and form a two-dimensional key space [68].

B. Stealth Transmission and Anonymous Communication

Optical steganography hides the signals in plain sight, and has significant potential to protect the privacy of user communications. One important application of optical steganography is to enable the design of anonymous communication systems.

Systems for anonymous communication aim to hide the sender identity from the recipients of the communication, as well as third parties in the network, such as Internet service providers (ISP). Users that desire anonymity include intelligence agencies, law enforcement, whistleblowers, political dissidents, journalists, businesses, and even ordinary Internet users wishing to avoid surveillance.

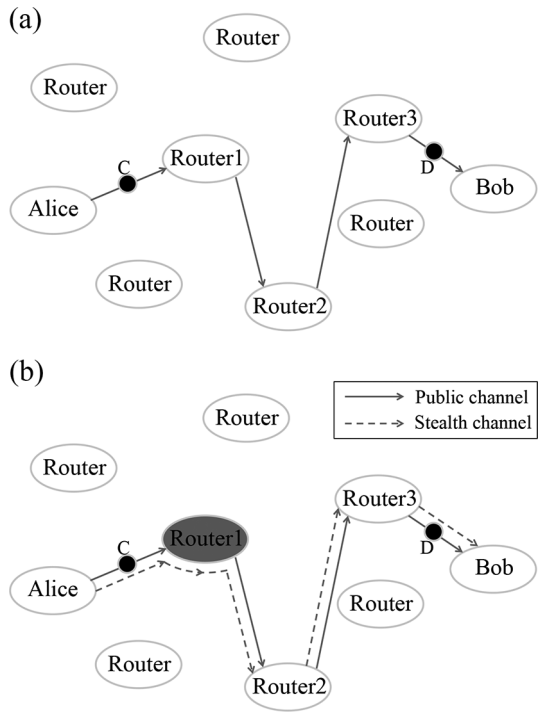


Fig. 10. Comparison of traditional Tor and Steganography assisted Tor (SAT).

We note that today's networks are easily susceptible to traffic analysis attacks that compromise user anonymity [71], [72]. For example, a network adversary, such as a malicious ISP or a router, can eavesdrop on user communications to infer the identity of communicating parties, thus violating user anonymity. Even the use of encryption techniques does not provide anonymity. Encryption only hides the contents of the communications, but does not protect the identity of the communicating parties.

The conventional approach for hiding the identities of the communicating parties is known as layered encryption, or in another words, the "Onion Router" (Tor) [73]–[75]. The Tor network is a deployed system for anonymous communication. If Alice wants to send a message to Bob, Alice chooses a path with routers/proxies (Fig. 10(a)). Layered encryption ensures that each router on the path learns the identity of only the previous router/node and the next router/node. Thus, no single router learns the identity of both the client and the destination. Even if one of the routers or links acts as an eavesdropper, user privacy is still preserved.

While the Tor network serves millions of users, its approach is not effective against traffic analysis. First, an attacker can perform traffic analysis of encrypted communications to learn the size and timings of the transmitted signals, since encryption does not hide the message size or timings. Second, if the eavesdropper can attack point C and D in the network of Fig. 10(b), the comparison and statistical analysis of message size and timing can reveal the correlation between the message flown through link C and link D. Thus, the message transmitter and receiver are exposed, breaking user anonymity.

The system can be effectively protected by optical steganography; in other words, steganography-assisted Tor (SAT). The function of optical steganography is to hide the very existence of signals. Either a certain link in the network can be hidden in the stealth channel or the stealth channel can pass through a router without being detected by the router. If the eavesdropper attacks point C and D, these two links can be hidden in the stealth channel. If the eavesdropper attacks router 1, the stealth channel can bypass router 1. Since the eavesdropper cannot detect the existence of the transmitted signal, he/she cannot do traffic analysis of the signal.

For efficiently deploying the stealth channel in the public network, the bandwidth of the stealth channel has to be considered. Because the capacity of the stealth channels is limited, it may be impractical to hide the entire data stream in the stealth channel. In this case, the stealth channel can hide a portion of messages in the data stream, while the remaining portion traverses the public channel. This approach perturbs the correlation function between the data streams at different links, and eavesdroppers are unable to de-anonymize users via traffic analysis. To qualitatively test the performance of an SAT system, the correlation function between data streams can be calculated as [75]:

$$r(d) = \frac{\sum_i ((x_i - \mu)(x'_{i+d} - \mu'))}{\sqrt{\sum_i (x_i - \mu)^2} \sqrt{\sum_i (x'_{i+d} - \mu')^2}} \tag{6}$$

where x_i is the data packet number measured in the i-th time window of a data stream, μ is the mean of $\{x_i\}$, x'_{i+d} is the packet number measured in the $i+d$-th time window of another data stream, μ' is the mean of $\{x'_{i+d}\}$, and d is the relative time delay between the two data streams. Future work is needed to optimize the scheme of choosing the packets for the stealth channel. The design of the scheme for a SAT network should aim to minimize the correlation function of two data streams in two connected links while consuming minimum capacity of the stealth channel.

IV. Conclusion

We proposed an optical encryption technique based on analog noise cancellation, a key generation method based on neuromorphic spike processing and optical stealth transmission techniques that hide the signals in the pre-existing noise. The proposed optical encryption technique protects signals with analog noise, which cannot be digitized, so without decrypting the signal when receiving the signals, the eavesdropper cannot recover the signal by post-processing techniques. Cancellation of the analog noise requires matching both the phase and the amplitude of the noise, which provides a two-dimensional key space for the encryption process. The optical key generation method generates encryption keys with a neuron spike processing system. The system converts public signals into the keys for encryption, with transmission of the public signals functioning as key distribution. Both optical encryption and key generation techniques process the lightwave signal in fiber-based components and thus do not emit any electromagnetic signature.

Optical stealth transmission enables signal transmission without detection, let alone decryption. Stealth transmission based on ASE noise uses amplifier noise to carry signals. Since this amplifier noise permeates most fiber optic networks, the eavesdropper cannot differentiate between stealth signals

and pure noise with either temporal or spectral domain analysis. In this way, optical stealth transmission (a.k.a. optical steganography) can effectively protect the privacy of optical data communication. Combined with layered encryption (Tor), optical steganography provides anonymous communication and defends the system against traffic analysis attacks.

REFERENCES

[1] M. P. Fok, Z. Wang, Y. Deng, and P. R. Prucnal, "Optical layer security in fiber-optic network," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 725–736, Sep. 2011.

[2] B. Wu, B. J. Shastri, and P. R. Prucnal, , B. Akhgar and H. Arabnia, Eds., "Secure communication in fiber-optic networks," in *Emerging Trends in ICT Security*. Waltham, MA, USA: Elsevier, 2014, pp. 173–183.

[3] 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.*, vol. 16, no. 3, pp. 897–899, Mar. 2004.

[4] J. H. Kim, Y. M. Jhon, Y. T. Byun, S. Lee, D. H. Woo, and S. H. Im, "All optical XOR gate using semiconductor optical amplifier without additional input beam," *IEEE Photon. Technol. Lett.*, vol. 14, no. 10, pp. 1436–1438, Oct. 2002.

[5] M. Jinno and T. Matsumoto, "Ultrafast all-optical logic operations in a nonlinear sagnac interferometer with two control beams," *Opt. Lett.*, vol. 16, no. 4, pp. 220–222, Feb. 1991.

[6] Q. Wang, G. Zhu, H. Chen, J. Jaques, J. Leuthold, A. B. Piccirilli, and N. K. Dutta, "Study of all-optical XOR using Mach-Zehnder interferometer and differential scheme," *IEEE J. Quantum Electron.*, vol. 40, no. 6, pp. 703–710, Jun. 2004.

[7] T. Fjelde, D. Wolfson, A. Kloch, B. Dagens, A. Coquelin, I. Guillemot, F. Gaborit, F. Poingt, and M. Renaud, "Demonstration of 20 Git/s all-optical logic XOR in integrated SOA-based interferometric wavelength converter," *Electron. Lett.*, vol. 36, no. 22, pp. 1863–1864, Oct. 2000.

[8] M. P. Fok and P. R. Prucnal, "Polarization effect on optical XOR performance based on four wave mixing," *IEEE Photon. Technol. Lett.*, vol. 22, no. 15, pp. 1096–1098, Aug. 2010.

[9] H. Soto, D. Erasme, and G. Guekos, "5-Gb/s XOR optical gate based on cross-polarization modulation in semiconductor optical amplifier," *IEEE Photon. Technol. Lett.*, vol. 13, no. 4, pp. 335–337, Apr. 2001.

[10] P. R. Prucnal, M. A. Santoro, and T. R. Fan, "Spread spectrum fiber-optic local area network using optical processing," *J. Lightw. Technol.*, vol. 4, no. 5, pp. 547–554, May 1986.

[11] C. S. Brès, Y.-K. Huang, I. Glesk, and P. R. Prucnal, "Scalable asynchronous incoherent optical CDMA [Invited]," *J. Opt. Netw.*, vol. 6, no. 6, pp. 599–615, Jun. 2007.

[12] Z. Jiang, D. E. Leaird, and A. M. Weiner, "Experimental investigation of security issues in O-CDMA," *J. Lightw. Technol.*, vol. 24, no. 22, pp. 4228–4234, Nov. 2006.

[13] X. Wang and N. Wada, "Experimental demonstration of OCDMA traffic over optical packet switching network with hybrid PLC and SSFGB en/decoders," *J. Lightw. Technol.*, vol. 24, no. 8, pp. 3012–3020, Aug. 2006.

[14] R. Matsumoto, T. Kodama, S. Shimizu, R. Nomura, K. Omichi, N. Wada, and K. I. Kitayama, "40G-OCDMA-PON system with an asymmetric structure using a single multi-port and sampled SSFBG encoder/decoders," *J. Lightw. Technol.*, vol. 32, no. 6, pp. 1132–1143, Mar. 2014.

[15] H. Mrabet, I. Dayoub, R. Attia, and S. Haxha, "Performance improving of OCDMA system using 2-D optical codes with optical SIC receiver," *J. Lightw. Technol.*, vol. 27, no. 21, pp. 4744–4753, Nov. 2009.

[16] Z. Wang, J. Chang, and P. R. Prucnal, "Theoretical analysis and experimental investigation on the security performance of incoherent optical CDMA Code," *J. Lightw. Technol.*, vol. 28, no. 12, pp. 1761–1769, Jun. 2010.

[17] G. D. VanWiggeren and R. Roy, "Communication with chaotic lasers," *Science*, vol. 279, no. 20, pp. 1198–1200, Feb. 1998.

[18] A. Argris, D. Syvridis, L. Larger, V. A. Lodi, P. Colet, I. Fischer, J. G. Ojalvo, C. R. Mira, I. Sso, L. Pesquera, and K. A. Shore, "Chaos-based communications at high bit rates using commercial fibre-optic links," *Nature*, vol. 438, no. 17, pp. 343–346, Nov. 2006.

[19] 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*, vol. 19, no. 24, pp. 23921–23931, Nov. 2011.

[20] L. Yang, L. Zhang, R. Yang, L. Yang, B. Yue, and P. Yang, "Chaotic dynamics of erbium-doped fiber laser with nonlinear optical loop mirror," *Opt. Commun.*, vol. 285, pp. 143–148, Sep. 2011.

[21] L. Larger and J. P. Goedgebuer, "Encryption using chaotic dynamics for optical telecommunications," *Comptes Rendus Phys.*, vol. 5, pp. 609–611, 2004.

[22] J. P. Goedgebuer, L. Larger, and H. Porte, "Optical cryptosystem based on synchronization of hyperchaos generated by a delayed feedback tunable laser diode," *Phys. Rev. Lett.*, vol. 80, no. 10, pp. 2249–2252, 1998.

[23] L. Larger, J. P. Goedgebuer, and F. Delorme, "Optical encryption system using hyperchaos generated by an optoelectronic wavelength oscillator," *Phys. Rev. E*, vol. 57, no. 6, pp. 6618–6624, Jun. 1998.

[24] M. Nazarathy, "Quantum key distribution over a fiber-optic channel by means of pulse position modulation," *Opt. Lett.*, vol. 30, no. 12, pp. 1533–1535, Jun. 2005.

[25] T. Honjo and H. Takesue, "Differential-phase quantum key distribution experiment using a series of quantum entangled photon pairs," *Opt. Lett.*, vol. 32, no. 9, pp. 1165–1167, May 2007.

[26] M. P. Chang, M. Fok, A. Hofmaier, and P. R. Prucnal, "Optical analog self-interference cancellation using electro-absorption modulators," *IEEE Microw. Wireless Compon.*, vol. 23, no. 2, pp. 99–101, Jan. 2013.

[27] M. P. Chang, C. L. Lee, B. Wu, and P. R. Prucnal, "Adaptive optical self-interference cancellation using a semiconductor optical amplifier," *IEEE Photon. Technol. Lett.*, vol. 27, no. 9, pp. 1018–1021, May 2015.

[28] M. P. Chang, N. Wang, B. Wu, and P. R. Prucnal, "A simultaneous variable optical weight and delay in a semiconductor optical amplifier for microwave photonics," *J. Lightw. Technol.* 2015, to be published.

[29] B. Wu, M. P. Chang, B. J. Shastri, Z. Wang, and P. R. Prucnal, "Analog noise protected optical encryption with two-dimensional key space," *Opt. Express*, vol. 22, no. 11, pp. 14568–14574, Jun. 2014.

[30] B. Wu, M. P. Chang, Z. Wang, B. J. Shastri, and P. R. Prucnal, "Optical encryption based on cancellation of analog noise," in *Proc. CLEO*, 2014, p. AW3P.5.

[31] G. P. Agrawal, "Chapter 6 optical amplifiers," in *Fiber-Optic Communication Systems*, 3rd ed. New York, NY, USA: Wiley-Interscience, 2002, pp. 230–231.

[32] R. Sarpeshkar, "Analog versus digital: Extrapolating from electronics to neurobiology," *Neural Comput.*, vol. 10, no. 7, pp. 1601–1638, 1998.

[33] D. Brunner, M. C. Soriano, C. R. Mirasso, and I. Fischer, "Parallel photonic information processing at gigabyte per second data rates using transient states," *Nat. Commun.*, vol. 4, p. 1364, Jan. 2013.

[34] D. Woods and T. J. Naughton, "Optical computing: Photonic neural networks," *Nature Phys.*, vol. 8, no. 4, pp. 257–259, Apr. 2012.

[35] A. N. Tait, M. A. Nahmias, Y. Tian, B. J. Shastri, and P. R. Prucnal, "Photonic neuromorphic signal processing and computing," in *Nanophotonic Information Physics*, ser. Nano-Optics and Nanophotonics, M. Naruse, Ed. Berlin/Heidelberg, Germany: Springer, 2014, pp. 183–222 [Online]. Available: http://dx.doi.org/10.1007/978-3-642-40224-1_8

[36] B. J. Shastri, A. N. Tait, M. A. Nahmias, B. Wu, B. Romeira, and P. R. Prucnal, "Bistable spiking circuit with grapheme excitable laser for cascadable photonic logic," in *Proc IEEE Summer Topicals Meeting Series*, Montreal, QC, Canada, Jul. 2014, pp. 108–109.

[37] B. J. Shastri, M. A. Nahmias, A. N. Tait, Y. Tian, B. Wu, and P. R. Prucnal, "Graphene excitable laser for photonic spike processing," in *Proc. IEEE Photon. Conf. (IPC)*, Sep. 2013, pp. 1–2 [Online]. Available: http://dx.doi.org/10.1109/IPCon.2013.6656424

[38] B. J. Shastri, M. A. Nahmias, A. N. Tait, B. Wu, and P. R. Prucnal, "SIMPEL: Circuit model for photonic spike processing laser neurons," *Opt. Express*, 2014 [Online]. Available: http://arxiv.org/abs/1409.7030, to be published

[39] B. J. Shastri, A. N. Tait, M. A. Nahmias, B. Wu, and P. R. Prucnal, "Coincidence detection with graphene excitable laser," in *Proc. Conf. Lasers Electro-Opt. (CLEO)*, San Jose, CA, USA, Jun. 2014, paper STu3I.5.

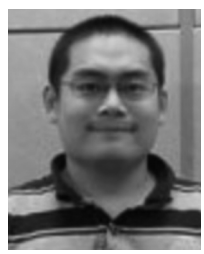
[40] B. J. Shastri, A. N. Tait, M. A. Nahmias, B. Wu, and P. R. Prucnal, "Spatiotemporal pattern recognition with cascadable grapheme excitable laser," in *Proc IEEE Photon. Conf. (IPC)*, San Diego, CA, USA, Oct. 2014, pp. 573–574, paper ThB1.2.

[41] B. J. Shastri, A. N. Tait, M. A. Nahmias, and P. R. Prucnal, "Photonic spike processing: Ultrafast laser neurons and an integrated photonic network," *IEEE Photon. Soc. Newslett.*, vol. 28, no. 3, pp. 4–11, Jun. 2014.

[42] A. N. Tait, M. A. Nahmias, B. J. Shastri, and P. R. Prucnal, "Broadcast-and-weight interconnects for integrated distributed processing systems," in *Proc. IEEE Opt. Interconnects Conf. (OI)*, Coronado Bay, CA, USA, May 2014, pp. 108–109, paper WA3.

[43] H. J. Caulfield and S. Dolev, "Why future supercomputing requires optics," *Nature Photon.*, vol. 4, no. 5, pp. 261–261, May 2010.

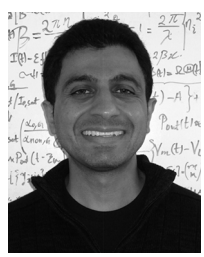
[44] B. Krauskopf, K. Schneider, J. Sieber, S. Wieczorek, and M. Wolfrum, "Excitability and self-pulsations near homoclinic bifurcations in semiconductor laser systems," *Optics Commun.*, vol. 215, no. 46, pp. 367–379, 2003.
[45] B. J. Shastri, M. A. Nahmias, A. N. Tait, Y. Tian, M. P. Fok, M. P. Chang, B. Wu, and P. R. Prucnal, "Exploring excitability in graphene for spike processing networks," in *Proc. IEEE Numerical Simulation of Optoelectron. Devices (NUSOD)*, Vancouver, BC, Canada, Aug. 2013, pp. 83–84, paper TuC5.
[46] S. Ibrahim, H. Ishikawa, T. Nakahara, and R. Takahashi, "A novel optoelectronic serial-to-parallel converter for 25-Gbps burst-mode optical packets," *Opt. Express*, vol. 22, no. 1, pp. 157–165, Jan. 2014.
[47] C. H. Kwok and C. Lin, "Polarization-insensitive all-optical NRZ-to-RZ format conversion by spectral filtering of a cross phase modulation broadened signal spectrum," *J. Lightw. Technol.*, vol. 12, no. 3, pp. 451–458, May–Jun. 2006.
[48] 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*, vol. 22, no. 1, pp. 954–961, Jan. 2014.
[49] B. Wu, Z. Wang, B. J. Shastri, Y. Tian, and P. R. Prucnal, "Phase-mask coved optical steganography based on amplified spontaneous emission noise," in *Proc. IEEE Photon. Conf.*, 2013, p. MG3.3.
[50] W. Stallings, "Chapter 1 Overview," in *Cryptography and Network Security Principles and Practice*, 5th ed. New York, NY, USA: Pearson, 2011, pp. 10–11.
[51] B. B. Wu, P. R. Prucnal, and E. E. Narimanov, "Secure transmission over an existing public WDM lightwave network," *IEEE Photon. Technol. Lett.*, vol. 18, no. 17, pp. 1870–1872, Sep. 2006.
[52] N. Bhargava, M. M. Sharma, A. S. Garhwal, and M. Mathuria, "Digital image authentication system based on digital watermarking," in *Proc. Int. Conf. Radar, Commun., Comput. (ICRCC)*, 2013, pp. 185–189.
[53] M. K. Dutta, A. Singh, and T. A. Zia, "An efficient and secure digital image watermarking using features from iris image," in *Proc. Int. Conf. Control Commun. Computi. (ICCC)*, 2013, pp. 451–456.
[54] V. Mehan, R. Dhir, and Y. S. Brar, "Joint watermarking and fingerprinting approach for colored digital images in double DCT domain," in *Proc. IEEE Int. Conf. Signal Process., Comput. Control (ISPCC)*, 2013, pp. 1–6.
[55] K. Raval and S. Zafar, "Digital watermarking with copyright authentication for image communication," in *Proc. Int. Conf. Intell. Syst. Signal Process. (ISSP)*, 2013, pp. 111–116.
[56] M. Hemahlathaa and C. Chellppan, "A feature-based robust digital image watermarking scheme," in *Proc. Int. Conf. Comput., Commun., Applicat. (ICCCA)*, 2012, pp. 1–5.
[57] R. K. Megalingam, M. M. Nair, R. Srikumar, V. K. Balasubramanian, and V. S. V. Sarma, "Performance comparison of novel, robust spatial domain digital image watermarking with the conventional frequency domain watermarking techniques," in *Int. Conf. Signal Acquisit. Process.*, 2010, pp. 349–353.
[58] M. Parasad and S. Koliwad, "A robust wavelet-based watermarking scheme for copyright protection of digital images," in *Proc. 2nd Int. Conf. Comput., Commun., Netw. Technol.*, 2010, pp. 1–9.
[59] Z. Wang and P. R. Prucnal, "Optical steganography over a public DPSK channel with asynchronous detection," *IEEE Photon. Technol. Lett.*, vol. 23, no. 1, pp. 48–50, Jan. 2011.
[60] 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*, vol. 21, no. 2, pp. 2065–2071, Jan. 2013.
[61] B. Wu, M. P. Chang, N. R. Caldwell, M. E. Caldwell, and P. R. Prucnal, "Amplifier noise based on optical steganography with coherent detection," *Coherent Opt. Phenom.*, vol. 2, pp. 13–18, 2014.
[62] B. Wu, A. N. Tait, M. P. Chang, and P. R. Prucnal, "WDM optical steganography based on amplified spontaneous emission noise," *Opt. Lett.*, vol. 39, no. 20, pp. 5925–5928, Oct. 2014.
[63] R. C. Steele, G. R. Walker, and N. G. Walker, "Sensitivity of optically preamplified receivers with optical filtering," *IEEE Photon. Technol. Lett.*, vol. 3, no. 6, pp. 545–547, Jun. 1991.
[64] B. Wu, B. J. Shastri, and P. R. Prucnal, "System performance measurement and analysis of optical steganography based on noise," *IEEE Photon. Technol. Lett.*, vol. 26, no. 19, pp. 1920–1923, Oct. 2014.
[65] N. A. Olsson, "Lightwave systems with optical amplifiers," *J. Lightw. Technol.*, vol. 7, no. 7, pp. 1071–1082, Jul. 1989.
[66] E. Desurvire, "Chapter 5 Gain, saturation and noise characteristics of erbium-doped fiber amplifiers," in *Erbium-Doped Fiber Ampplifiers, Principle and Applications*, 2nd ed. Hoboken, NJ, USA: Wiley-Interscience, 2002, pp. 355–357.
[67] E. Desurvire, "Analysis of noise figure spectral distribution in erbium doped fiber amplifiers pumped near 980 and 1480 nm," *Appl. Opt.*, vol. 29, no. 21, pp. 3118–3125, July 1990.
[68] B. Wu, Z. Wang, B. J. Shastri, Y. Tian, and P. R. Prucnal, "Two dimensional encrypted optical steganography based on amplified spontaneous emission noise," in *Proc. CLEO*, 2013, p. AF1H.5.
[69] I. B. Djordjevic, A. H. Saleh, and F. Kuppers, "Design of DPSS based fiber Bragg grating and their application in all-optical encryption, OCDMA, optical steganography, and orthogonal-division multiplexing," *Opt. Express*, vol. 22, no. 9, pp. 10882–10897, May 2014.
[70] M. A. Islam and M. S. Alam, "Design optimization of equiangular spiral photonic crystal fiber for large negative flat dispersion and high birefringence," *J. Lightw. Technol*, vol. 30, no. 22, pp. 3545–3551, Nov. 2012.
[71] F. Zhang, W. He, and X. Liu, "Defending against traffic analysis in wireless networks through traffic reshaping," in *Proc. 31st Int. Conf. Distrib. Comput. Syst.*, Minneapolis, MN, USA, Jun. 2011, pp. 593–602.
[72] Y. Lu and Y. Zhu, "Correlation-based traffic analysis on encrypted VoIP traffic," in *Proc. 2nd Int. Conf. Netw. Security, Wireless Commun. Trusted Comput.*, Wuhan, China, Apr. 2010, pp. 45–48.
[73] D. Goldschlag, M. Reed, and P. Syverson, "Onion routing," *Commun. ACM*, vol. 42, no. 2, pp. 39–41, Feb. 1999.
[74] M. G. Reed, P. F. Syverson, and D. M. Goldschlag, "Anonymous connections and onion routing," *IEEE J. Sel. Areas Commun.*, vol. 16, no. 4, pp. 482–494, May 1998.
[75] P. Mittal, F. Olumofin, C. Troncoso, N. Borisov, and I. Goldberg, "PIR-Tor: scalable anonymous communication using private information retrieval," in *Proc. USENIX Security Symp.* [Online]. Available: https://www.usenix.org/conference/usenix-security-11/pir-tor-scalable-anonymous-communication-using-private-information
[76] B. N. Levine, M. K. Reiter, C. Wang, and M. Wright, "Timing attacks in low latency mix systems," *Financ. Cryptogr. Lecture Notes Comput. Sci.*, vol. 3110, pp. 251–265, 2004.



Ben Wu received the B.Sci. (with distinction) in the Optoelectronics Department from Nankai University, Tianjin, China, in 2008. He is currently a Ph.D. candidate at Princeton University, Department of Electrical Engineering.

He was a Research Intern in the summer of 2008 in Institute of Modern Optics, Nankai University. His current research interests include optical stealth transmission, optical encryption and photonic ultra-fast signal processing. He has published a chapter in the book: *Emerging Trends in ICT Security* (Waltham, MA: Elsevier, 2013).

Mr. Wu has the following awards: 2014 Wu Prize for Excellence in Princeton University, 2013 Excellence in Teaching, 2009 Graduate Student Fellowship, 2008 Excellent Graduation Thesis (top one out of sixty students).

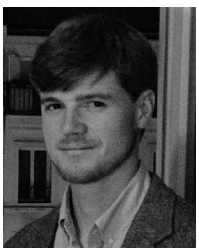


Bhavin J. Shastri (S'03–M'11) received the Honors B.Eng. (with distinction), M.Eng., and Ph.D. degrees in electrical engineering from McGill University, Montreal, QC, Canada, in 2005, 2007, and 2011, respectively.

He is currently a Banting Postdoctoral Fellow at Princeton University, Princeton, NJ, USA. His research interests include photonic cortical information processing (ultrafast cognitive computing), optoelectronic devices, machine learning, and computer vision.

Dr. Shastri has garnered the following research awards: Banting Postdoctoral Fellowship from the Government of Canada through the Natural Sciences and Engineering Research Council of Canada (NSERC), 2012 D. W. Ambridge Prize for the top graduating Ph.D. student, nomination for the 2012 Canadian Governor General's Gold Medal, IEEE Photonics Society 2011 Graduate Student Fellowship, 2011 NSERC Postdoctoral Fellowship, 2011 SPIE Scholarship in Optics and Photonics, a Lorne Trottier Engineering Graduate Fellow, and a 2008 Alexander Graham Bell Canada Graduate Scholarship from NSERC. He was the recipient of the Best Student Paper Awards at the 2010 IEEE Midwest Symposium on Circuits and Systems (MWSCAS), the co-recipient of the Silver Leaf Certificate at the 2008 IEEE Microsystems and Nanoelectronics Conference (MNRC), the 2004 IEEE Computer Society Lance Stafford Larson Outstanding Student Award, and the 2003 IEEE Canada Life Member Award. Dr. Shastri was the President/Co-Founder of the McGill OSA Student Chapter.

Prateek Mittal (S'07–M'13) obtained his Ph.D. in electrical and computer engineering from University of Illinois at Urbana-Champaign in 2012. He is an Assistant Professor in the Department of Electrical Engineering at Princeton University. His research aims to build secure and privacy-preserving communication systems. His research interests include the domains of privacy enhancing technologies, trustworthy social systems, and Internet/network security. His work has influenced the design of several widely used anonymity systems, and is the recipient of several awards including an ACM CCS outstanding paper. He served as the program co-chair for the HotPETs workshop, in 2013 and 2014. Prior to joining Princeton University, he was a postdoctoral scholar at University of California, Berkeley.



Alexander N. Tait (S'11) received the B.Sci.Eng. (Honors) in electrical engineering in 2012 from Princeton University, Princeton, NJ, USA, where he is currently working toward the Ph.D. degree in electrical engineering in the Lightwave Communications Group, Department of Electrical Engineering.

He was a Research Intern for the summers of 2008–2010 at the Laboratory for Laser Energetics, University of Rochester, Rochester, NY and an undergraduate researcher for the summers of 2011–2012 at the MIRTHE Center, Princeton University, Princeton, NJ. His research interests include photonic devices for nonlinear signal processing, integrated systems, neuromorphic engineering, and hybrid analog–digital signal processing and computing.

Mr. Tait is a Student Member of the IEEE Photonics Society and the Optical Society of America (OSA). He is a recipient of the National Science Foundation Graduate Research Fellowship. He is a co-recipient of the Optical Engineering Award of Excellence from the Department of Electrical Engineering at Princeton. He has authored 2 papers and a book chapter and co-authored 8 journal papers appearing in Optics Letters, the Journal of Applied Physics, and others.

Paul R. Prucnal (S'75–M'79–SM'90–F'92) received the A.B. degree from Bowdoin College (summa cum laude), with Highest Honors in math and physics, where he was elected to Phi Beta Kappa. He then received the M.S., M.Phil., and Ph.D. degrees from Columbia University, where he was elected to the Sigma Xi honor society.

He was an Assistant and then tenured Associate Professor at Columbia from 1979 until 1988, when he joined Princeton University, Princeton, NJ, as a Professor of Electrical Engineering. He has held visiting faculty positions at the University of Tokyo and University of Parma. From 1990 to 1992, he served as the Founding Director of Princeton's Center for Photonics and Optoelectronic Materials, and is currently the Director of the Center for Network Science and Applications. He is widely recognized as the inventor of the "Terahertz Optical Asymmetric Demultiplexer," an ultrafast all-optical switch, and has done seminal research in the areas of all-optical networks and photonic switching. His pioneering research on optical CDMA in the mid-1980s initiated a new research field where more than 1000 papers have now been published worldwide. With support from the Defense Advanced Research Projects Agency in the 1990s, his group was the first to demonstrate an all-optical 100-Gb/s photonic packet switching node and optical multiprocessor interconnect. His recent work includes the investigation of linear and nonlinear optical signal processing techniques to provide high-speed data confidentiality in communications networks. He has published over 250 archival journal papers and holds 17 patents.

Prof. Prucnal is an Area Editor of the IEEE TRANSACTIONS ON COMMUNICATIONS for optical networks, and was Technical Chair and General Chair of the IEEE Topical Meeting on Photonics in Switching in 1997 and 1999, respectively. He is a Fellow of IEEE with reference to his work on optical networks and photonic switching, a Fellow of the OSA, and a recipient of the Rudolf Kingslake Medal from the SPIE, cited for his seminal paper on photonic switching. In 2006, he was awarded the Gold Medal from the Faculty of Physics, Mathematics and Optics from Comenius University in Slovakia, for his contributions to research in photonics. In 2004, 2006, and 2008, he received Princeton Engineering Council Awards for Excellence in Teaching, in 2006 he received the University Graduate Mentoring Award, and in 2009 the Walter Curtis Johnson Prize for Teaching Excellence in Electrical Engineering, as well as the Distinguished Teacher Award from Princeton's School of Engineering and Applied Science. He is editor of the book, *Optical Code Division Multiple Access: Fundamentals and Applications*, published by Taylor and Francis in 2006.