Steganographic Communication via Spread Optical Noise: A Link-Level Eavesdropping Resilient System

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

***Abstract*—We are witnessing a rising concern over communication security and privacy. Conventional cryptography techniques encrypt data into unreadable codes, but still expose the existence of communications through metadata information (e.g., packet timing and size). In contrast, we propose a steganographic communication scheme adopting a novel combination of the intrinsic optical noise and a unique signal spreading technique to hide the existence of optical communications, i.e., optical steganography. We experimentally implement a prototype steganographic communication system, which requires zero cover-signal overhead to enable a stealth communication channel over the existing communication infrastructure. Both the frequency and time-domain characterizations of our prototype implementation verify the feasibility of our approach. We also demonstrate the first practical steganographic communication that provides reliable communication performances between real computers at the application layer (200–300 Mb/s file transfer rate and 25–30 Mb/s Internet data rate) over long-distance optic fibers (25–50 km). Additional bit-error-rate measurements illustrate negligible channel interference between the public and stealth communications (less than 1 dB power penalty). We further quantitatively demonstrate that the eavesdropper's chance of matching system parameters to effectively recover the stealth signal is 2^{-10} by random guessing, and that the eavesdropper's ability of detecting the stealth signal hidden in the transmission channel is strictly limited close to a random guess. Our steganographic communication scheme provides an attractive foundation for mitigating eavesdropping at the link level; thus, paving the way for future privacy-enhancing technologies using the physical layer characteristics of communication links.**

***Index Terms*—Communication security and privacy, optical fiber communications, optical steganography.**

Manuscript received May 31, 2018; revised August 8, 2018 and September 12, 2018; accepted September 12, 2018. Date of publication September 27, 2018; date of current version November 2, 2018. This work was supported by the National Science Foundation under Grant ECCS-1642962. *(Corresponding author: Philip Y. Ma.)*

P. Y. Ma, P. Mittal, and P. R. Prucnal are with the Department of Electrical Engineering, Princeton University, Princeton, NJ 08544 USA (e-mail: yechim@princeton.edu; pmittal@princeton.edu; prucnal@princeton.edu).

B. Wu was with the Department of Electrical Engineering, Princeton University, Princeton, NJ 08544 USA. He is now with the Department of Electrical and Computer Engineering, Rowan University, Glassboro, NJ 08028 USA (e-mail: wub@rowan.edu).

B. J. Shastri was with the Department of Electrical Engineering, Princeton University, Princeton, NJ 08544 USA. He is now with the Department of Physics, Engineering Physics and Astronomy, Queen's University, Kingston, ON K7L 3N6, Canada (e-mail: shastri@ieee.org).

A. N. Tait was with the Department of Electrical Engineering, Princeton University, Princeton, NJ 08544 USA. He is now with the National Institute of Standards and Technology, Boulder, CO 80305 USA (e-mail: atait@ieee.org).

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/JLT.2018.2872422

I. Introduction

OUR communications are dominated by optical networks, in which data is encoded onto light to transmit information. Unfortunately, information transmitted through optical networks can be readily collected by tapping into fiber-optic cables with off-the-shelf fiber hacking devices [1], [2]. Such vulnerability is shared among optical links (e.g., operated by Internet service providers) carrying the phone and Internet traffic [3], private networks (e.g., data centers) inter-connected by optical networking technologies [4], and the Internet backbone (e.g., undersea fiber-optic cables) that shuttle communications between continents and servers [5], [6].

As a result, optical networks rely heavily on cryptography to encode data with difficult-to-compute ciphers to prevent access by potential adversaries. Cryptography, while keeping data (computationally) confidential, does not hide the encoded messages themselves. Eavesdroppers know that a message is being delivered, and may eventually crack the encryption and uncover the message provided that enough storage and computing resources are available. Therefore, network surveillance activities are fueling urgent concerns over data privacy in communications, especially under the revelation of the Tempora program buffering data for three days and metadata for thirty days [7], and the Marina program storing vast amounts of metadata up to one year [8]. To make matters even worse, the metadata information that cannot be protected by cryptography (e.g., packet timing and size) may otherwise be used for malicious activities such as traffic analysis attacks [9]–[12], and website/device fingerprinting attacks [13]–[17].

The research community has investigated many information hiding technologies to mitigate signal interception and data eavesdropping, including the spread spectrum radio (for wireless communications) [18]–[20], anonymous communication systems (to hide user identities) [21]–[23], and digital watermarking techniques (for authentication purpose) [24]–[27]. As far as communication concealment is concerned, an important sub-discipline of information hiding is *steganography* where the secret information embedded within the publicly known cover-medium can be extracted by no one but the intended recipient [28]. Major breakthroughs have been made in digital steganography where secret data can be hidden within pixels, sound samples, as well as text messages [29]–[31], and network steganography where secret information can be placed in the header of a TCP/IP datagram [32]–[34]. However, these techniques are mainly

limited by their low throughput and considerable cover-medium overhead [35].

In the context of optical communications, *optical steganography* was proposed as a form of analog steganography to enable steganographic communications over optical transmission channels that can be publicly accessed by eavesdroppers [36]. These initial schemes, using either conventional long-distance fiber spools [37]–[39], or chirped fiber Bragg gratings (CFBG) [40]–[42], spread the stealth signal in the time domain to reduce its power level below the noise floor. In order to cover the existence of the low power stealth signal in the frequency domain, additional high power public (cover) signal has to co-exist at the same channel bandwidth, which not only restricts their practical usage in real optical networks where bandwidth resources are limited, but also requires very delicate channel separation techniques to limit the mutual influence between channels. Moreover, the addition of the stealth channel may easily expose itself by changing the transmission channel power level since the stealth channel was created by a separate laser source.

Recently, another optical steganography scheme established a stealth communication channel using the widely existing amplified spontaneous emission (ASE) noise as the optical carrier [43]–[45]. While embedding data in the ASE noise enables the stealth signal to better emulate the noise behavior, this approach required phase modulation and Mach-Zehnder interferometer (MZI) to prevent information leakage in the time domain (leveraging the optical path difference of MZI as an one-dimensional key). Unfortunately, their sensitivity to temperature and mechanical vibrations led to extremely unstable data transmission (as acknowledged by authors in [43]). Furthermore, the chance of exposing the stealth channel still persists since the stealth channel used a separate erbium-doped fiber amplifier (EDFA) as the ASE noise source.

In this paper, we extend our preliminary work [46] and summarize our contributions to optical steganography as follows:

- We propose an optical steganography paradigm, in which (a) data is carried by part of the innate noise of an optical communication channel, i.e., ASE noise, and (b) the data-carrying ASE noise is stretched temporally by a unique signal spreading function performed by CFBG (Section II). In contrast to prior works utilizing either signal spreading [36]–[42] or optical noise [43]–[45] *alone*, the novel *combination* of them allows us to not only transmit the data-carrying ASE noise in a noise-like form, but also minimize its difference against the part of ASE noise not carrying data to the point where they become virtually indistinguishable (see proof in subsequent sections). The fact that our scheme exploits the ubiquitous channel noise instead of a dedicated public signal enables the steganographic communication with zero cover-signal overhead.
- We experimentally implement a prototype steganographic communication system where a stealth channel for secret users can be established using the existing communication infrastructure for public users, and perform system characterizations in both the frequency and time domains to validate the feasibility of our approach (Section III). Our implementation (a) provides flexible channel selections by lifting the restriction that the public and stealth channels have to stay on the same bandwidth (as in [36]–[42]), (b) supports stable data-carrying ASE noise transmission by replacing environment-sensitive setup (adopted in [43]–[45]) with simpler direct detection scheme, (c) overcomes the security vulnerability of preceding cases where the stealth channel operation may easily affect the transmission channel power by introducing the public channel ASE noise into the stealth channel without having the stealth channel itself generate the optical carrier.
- We demonstrate the first practical steganographic communication between *real computers* that exercises the full network stack over long-distance (25–50 km) fiber-optic cables (Section IV). The data rate for the secret users *at the application layer* reaches 200–300 Mbps for local file transfer and 25–30 Mbps for Internet browsing. As opposed to prior works that delivered only pseudo-random bit sequence (PRBS), we are the first to show a physical-layer approach that is fully compatible with upper-layer hierarchy and is ready for direct deployment to today's communication networks. Moreover, the bit-error-rate (BER) measurements where the public and stealth channels impose less than 1 dB power penalty upon each other illustrates negligible mutual influence between channels (i.e., achieving independent channel operations).
- We quantitatively analyze the eavesdropper's difficulties to recover the stealth signal by finding the system parameters used to generate the stealth signal, i.e., the ASE noise bandwidth used to carry the stealth data and the CFBG dispersion parameter used to spread the data-carrying ASE noise (Section V). Our conservative analysis considers a semi-infinite two-dimensional key space where the chance for the eavesdropper to effectively match both of these two system parameters (to obtain a recovered stealth signal whose signal-to-noise ratio (SNR) is above 1) is 2^{-10} by random guessing.
- We quantitatively evaluate the steganographic communication security against an eavesdropper who aims to detect any stealth signal being transmitted by statistically analyzing the transmission channel signal (Section VI). We are the first to follow the formal information-theoretic treatment of steganography by analytically demonstrating our steganographic communication system to be ϵ-*secure* (approaching perfect indistinguishability given a sufficiently large signal spreading or data rate). We further employ support vector machines (SVMs) to empirically demonstrate the eavesdropper's ability to distinguish the stealth signal hidden in the transmission channel is close to a random guess.

II. Steganographic Communication Approach

Our steganographic communication system considers a pair of sender and recipient (e.g., real computers) connected by a fiber-optic link (i.e., a transmission channel). In conventional optical communications, the sender's transmitter and the recipient's receiver are mainly responsible for data modulation and

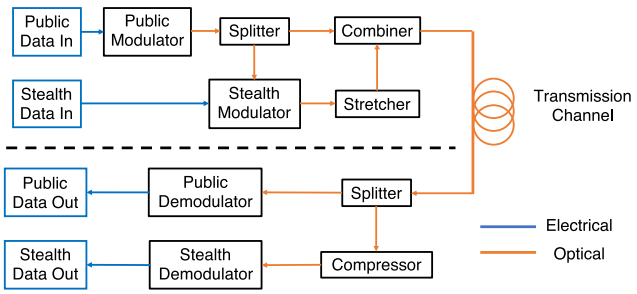

Fig. 1. Schematic illustration of the steganographic communication system.

demodulation (see Appendix A for analytic discussions); our approach augments these functionalities to perform steganographic encoding and decoding on the stealth data.

A. Approach Overview

We propose *spread optical noise*, a novel combination of the intrinsic optical channel noise and a unique signal spreading technique, to enable the steganographic communication.

Fig. 1 shows the schematic illustration of the proposed steganographic communication system. On one hand, the public channel (Public Data In → Public Data Out) only performs simple data modulation and demodulation. On the other hand, a splitter is used at the transmitter to separate part of the public channel background ASE noise into the stealth channel (Stealth Data In → Stealth Data Out). The stealth signal is generated by modulating the stealth data onto this particular ASE noise, and temporally stretching the data-carrying ASE noise by CFBG based on its dispersion effect (see Appendix B for detailed descriptions). We put the stealth signal back to the transmission channel by a combiner. Upon receiving the transmission channel signal, another splitter can be used to filter out the same ASE noise for the stealth channel, and a compressor will recover the data-carrying ASE noise for the stealth demodulator. The successful reconstruction of the stealth signal at the receiver, therefore, depends on if the spread data-carrying ASE noise can be well separated from the ASE noise not carrying data and compressed in the exact opposite way it was spread before.

B. System Parameters

There are two critical system parameters (i.e., the key) associated with this spread optical noise approach:

- *ASE noise bandwidth* used to carry the stealth data: We adopt the ubiquitous ASE noise in the optical channel, but only use part of the ASE noise to carry the stealth data. The stealth channel ASE noise bandwidth can be any interval within the total ASE noise spectral band (selected by CFBG bandwidth in our scheme).
- *CFBG dispersion parameter* used to spread the data-carrying ASE noise: We adopt CFBG as the stretching element that determines how much signal spreading is applied to the data-carrying ASE noise, and its dispersion parameter can literally take any value ranging from zero to infinity.

III. System Implementation & Characterizations

A. System Implementation

Fig. 2 illustrates the experimental setup of the prototype steganographic communication system.

At the transmitter, the public user employs an intensity modulator (IM) to modulate public data onto the optical carrier generated by a laser diode (LD) (whose central wavelength is at 1550 nm). EDFA1 amplifies this public signal and generates its background ASE noise. CFBG1 (whose dispersion is 4.1 ns/nm and whose bandwidth is 0.9 nm wide centered at 1530 nm) reflects part of the public channel ASE noise to the stealth channel, while letting the rest of the ASE noise plus the public signal go through to the coupler. EDFA2 amplifies the ASE noise entering the stealth channel for intensity modulating stealth data onto it. CFBG2 has the same bandwidth, dispersion parameter, and orientation as CFBG1, thus performing signal spreading to the data-carrying ASE noise. EDFA3 tunes the stealth channel power to the coupler, which combines the stealth channel with the public channel in the transmission channel. EDFA4 in the transmission channel is used to enable signal transmission over long-distance optic-fibers.

At the receiver, CFBG3 shares the same bandwidth and dispersion parameter as CFBG1 and CFBG2, but is placed in the opposite orientation against the other two. Upon receiving the transmission channel signal, therefore, CFBG3 separates the stealth signal (output from the port3 of circulator3) from the public signal plus the pure ASE noise (going through CFBG3), and compensates the signal spreading for the data-carrying ASE noise simultaneously. The transmitter requires two CFBGs because we need an ASE noise bandwidth selection before stealth data modulation, while the signal spreading cannot be performed without a data-carrying ASE noise. EDFA5 amplifies the relatively weak data-carrying ASE noise, and a photo-detector (PD) is used to demodulate the public and stealth data, respectively.

B. System Characterizations

We then adopt both the frequency and time domain characterizations to verify our prototype implementation achieves the desired steganographic communication purpose.

Fig. 3 shows the spectrum analysis of the steganographic communication system. Fig. 3(i) shows the spectrum before channel separation, which corresponds to a public channel peak at 1550 nm with the pure ASE noise background. Fig. 3(ii) is the public channel spectrum after the ASE noise around 1530 nm being filtered out by CFBG1 as the stealth channel optical carrier. Fig. 3(iii) is the stealth channel spectrum, exhibiting a power surge around 1530 nm that matches its absence in Fig. 3(ii). Fig. 3(iii) has a weak ASE noise background because this spectrum is taken after EDFA3. Fig. 3(iv) is the transmission channel spectrum after coupling both the public and stealth channels, which looks as if the stealth channel does not exist. This is achieved by coordinating EDFA2 and EDFA3 to balance the optical power entering and leaving the stealth channel, so that the stealth channel will not be exposed in the frequency domain.

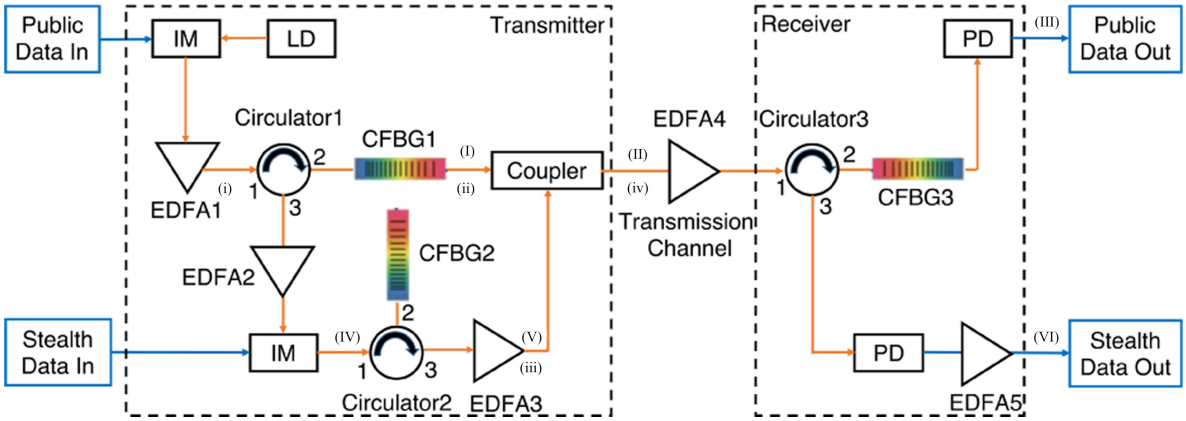

Fig. 2. Experimental setup of the steganographic communication system. Labels (i)-(iv), (I)-(VI) correspond to those in Fig. 3 and Fig. 4.

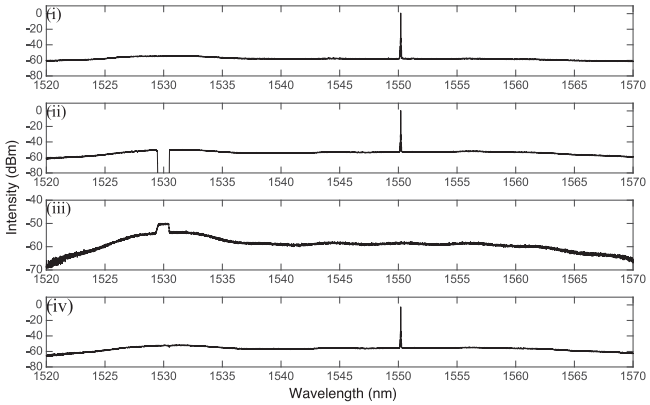

Fig. 3. Wavelength spectrum of (i) the public channel plus the pure ASE noise background before CFBG1, (ii) the public channel plus the ASE noise with the stealth channel taken out after CFBG1, (iii) the stealth channel plus the pure ASE noise added after EDFA3, (iv) the public channel plus the stealth channel and the pure ASE noise in the transmission channel after coupler.

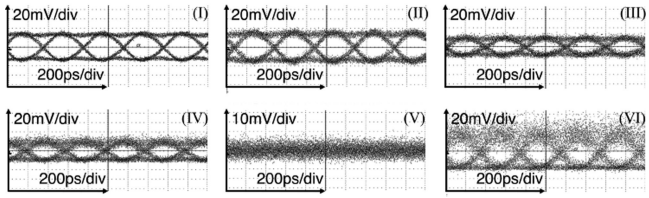

Fig. 4. Eye diagrams of (I) the public signal at the transmitter, (II) the transmission channel signal, (III) the public signal at the receiver, (IV) the stealth signal before signal spreading at the transmitter, (V) the stealth signal after signal spreading at the transmitter, (VI) the stealth signal after dispersion compensation at the receiver.

Fig. 4 presents the eye diagram measurements of the steganographic communication system. Fig. 4(I) is the public signal at the transmitter, and Fig. 4(IV) is the stealth signal before being spread by CFBG2. The stealth signal after being spread by CFBG2, as shown in Fig. 4(V), only contributes to the noise of the transmission channel signal in Fig. 4(II). In that case, the transmission channel signal appears for the eavesdropper to contain only the public signal while in fact the stealth signal is embedded as part of its noise. Fig. 4(III) and 4(VI) suggest both the public and stealth signals are well-received at the receiver.

IV. Communication Performance

A. System Configurations

We further test the communication performance of our steganographic communication system (physically shown in Fig. 5). We connect the IM-PD pair to two media converters (MCs), which interface the steganographic communication system with two computers through Ethernet cables. We place a desktop (2.8 GHz Intel Pentium 4 CPU) at the transmitter, and a laptop (2.9 GHz Intel Core i7-3520M CPU) at the receiver. The two computers can switch between two channels by connecting the MCs with the IM/PD pair in different channels. There is a back-to-back connection between these two MCs to complete the communication loop since our steganographic link is unidirectional for proof-of-concept purpose. Bidirectional steganographic communication can be achieved by replicating the same system implementation in the reverse direction. We share the Wireless Internet Connection on the laptop with the Local Area Connection it has with the steganographic communication system. In this case, *the desktop has its only connection with the outside world through the steganographic communication link with the laptop.*

B. Data Rate Measurements

Since the stealth channel ASE noise has a bandwidth of 115.3 GHz, Gbps data can be easily handled at the physical layer of our system (e.g., eye diagrams in Fig. 4 are measured with 3 Gbps PRBS). For the sake of actual deployment between real computers, we are more concerned with the data rate at the application layer (i.e., the upstream data rate from desktop to laptop). We first measure the data rate when locally transferring a large file (size of 3.09 GB) from the desktop to the laptop, and there exists an 1000 Mbps electrical I/O speed bottleneck at the network interface card (of both computers). We then measure the data rate when browsing the Internet at the desktop, and there exists an 100 Mbps electrical I/O speed bottleneck at the wireless network interface card (of the laptop). We summarize the communication performance of the public and stealth channels in Table I.

As for the public channel, it has 363.5 Mbps local transfer rate and 50.20 Mbps Internet upload rate, which sets a benchmark

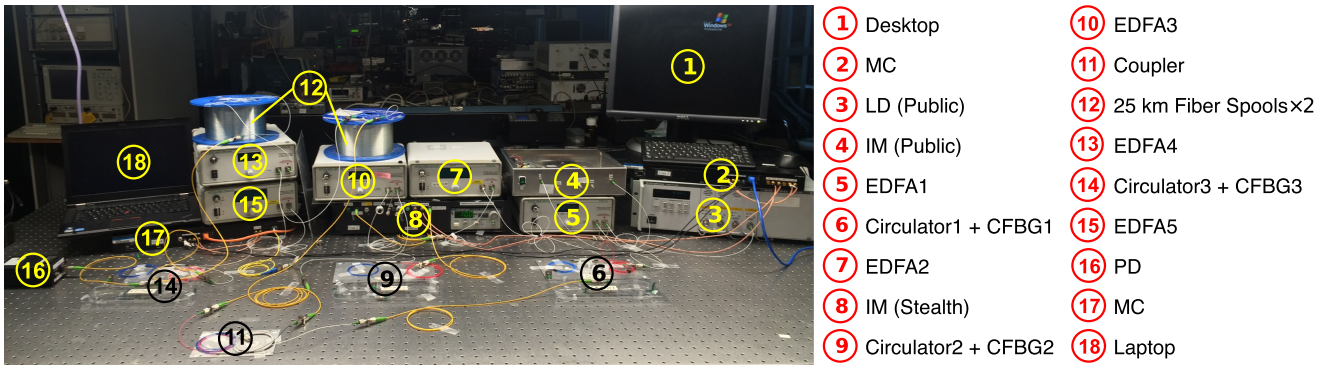

Fig. 5. Physical view of the steganographic communication system.

TABLE I
COMMUNICATION PERFORMANCE OF THE STEGANOGRAPHIC COMMUNICATION SYSTEM

Channel	Public Channel	Stealth Channel	
Transmission Distance	50-km	25-km	50-km
Local Transfer Rate	363.5 Mbps	257.5 Mbps	237.7 Mbps
Internet Upload Rate	50.20 Mbps	24.83 Mbps	24.17 Mbps

for comparison with those values of the stealth channel. As for the stealth channel, we consider two practical cases here:

- Steganographic communication over 25 km without a transmission channel EDFA: This case aims to demonstrate the delivery sustainability of the stealth signal over long distances. The data rate is 257.5 Mbps for local file transfer and 24.83 Mbps for Internet upload. The performance degradation is due to the fact that we are using the ASE noise as the optical carrier, which highly affects the stealth signal SNR.
- Steganographic communication over 50 km with a transmission channel EDFA: This case aims to investigate how a relaying amplifier may extend the transmission distance and affect the communication performance. The data rate slightly decreases to 237.7 Mbps for local file transfer and 24.17 Mbps for Internet upload, which can be attributed to the additional pure ASE noise generated in the same ASE noise bandwidth that carries the stealth data.

We thus confirm that our prototype steganographic communication system can deliver reliable communication performance for both public and stealth users over most Local Area Networks (<10 km) and Metropolitan Area Networks (<50 km). It is worth mentioning the trade-off between performance and security: while the stealth channel has a comparatively worse communication performance than the public channel, it provides the stealth signal with additional protection against eavesdropping. *To the best of the author's knowledge, this is the first demonstration of an optical steganographic communication link that practically works between two real computers over long-distance optic-fibers.*

C. Bit-Error-Rate Measurements

Meanwhile, we are also concerned with the BER (the number of error bits received over the total number of bits received at the laptop) of the public and stealth channels, which is shown in Fig. 6. Both channels can be operated within the Forward Error Correction (FEC) limit. The public channel reaches a BER of 10^{-9} with -5 dBm received signal power while the stealth channel reaches a BER of 10^{-6} with 0 dBm received signal power. Given the same BER, the stealth channel has an 8 dB power penalty when compared to the public channel. This is simply because the stealth channel has a lower SNR, and requires higher power to reach the same BER (this is another manifestation of the trade-off between performance and security as mentioned before).

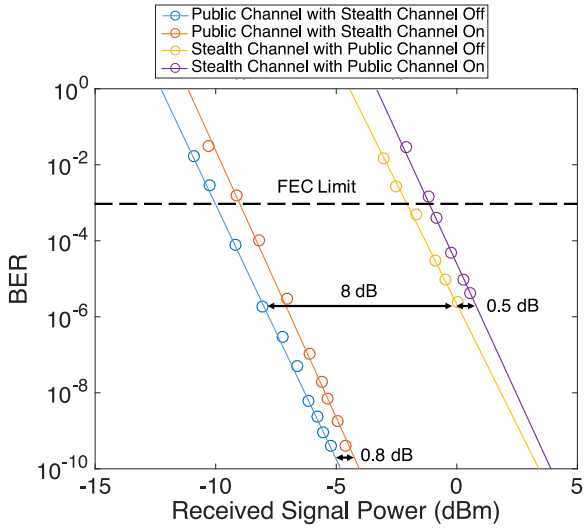

Fig. 6. BER measurements of the steganographic communication system.

The other important aspect of this BER measurements is the mutual influence between the public and stealth channels. Turning on the stealth channel places a 0.8 dB power penalty upon the public channel, while turning on the public channel imposes a 0.5 dB power penalty upon the stealth channel. The slight BER degradation of individual channel results mainly from the variations in the transmission channel signal power distribution, which in turn affect the gain distribution of the transmission channel EDFA (i.e., EDFA4). In essence, less than 1 dB power penalties evidence that the public and stealth channels do not interfere with each other, owing to our steganographic design

where the bandwidths of public and stealth channels do not need to overlap.

V. Security Analysis of System Parameters

Conventional steganography model respects the prudent "Kerckhoffs's principle" (in cryptography) that the security of a system relies sorely on the secrecy of its key [47]. Therefore, the system parameters used in our implementation, which form a semi-infinite two-dimensional key space, can be assumed to be secure against eavesdroppers. Nevertheless, we recognize in our particular scenario that the eavesdropper is capable of acquiring necessary (analog) signal processing equipment, e.g., a tunable bandwidth selector for locating the ASE noise bandwidth, and a tunable dispersion compensator for compressing the stealth signal.

We hereby discuss how difficult it is for an eavesdropper to recover the stealth signal by matching his/her own ASE noise bandwidth $\Delta\nu_{eav}$ and dispersion parameter D_{eav} with the correct ASE noise bandwidth $\Delta\nu_{CFBG}$ that carries the stealth data and the correct CFBG dispersion parameter D_{CFBG} used to spread the data-carrying ASE noise. We quantify the eavesdropper's stealth signal recovery effectiveness using the ratio of the recovered stealth signal $SNR_{recovered}$ achieved by the eavesdropper against the target stealth signal SNR_{target} achieved by the legitimate receiver. We only present our results here, but provide detailed derivations in Appendix C.

A. ASE Noise Bandwidth Matching

We first focus on the eavesdropper's efforts in matching the ASE noise bandwidth. The eavesdropper faces the challenge of selecting a $\Delta\nu_{eav}$ that (a) is as wide as $\Delta\nu_{CFBG}$, (b) overlaps as much as $\Delta\nu_{CFBG}$. However, if $\Delta\nu_{eav}$ is too narrow, $\Delta\nu_{Overlap}$ does not contribute much to the recovered signal power; conversely, if $\Delta\nu_{eav}$ is too wide, it will contribute significantly to the recovered noise power even though there is a higher chance of bandwidth overlapping. Fig. 7(a) plots $SNR_{recovered}/SNR_{target}$ versus the spectral range $\Delta\lambda_{eav}$ and its position λ_{eav}, with a target $\Delta\lambda_{CFBG} =$ 0.9 nm located at $\lambda_{CFBG} = 1530$ nm. $\Delta\nu_{Overlap}$ is non-zero only when $\Delta\lambda_{eav}$ overlaps with the target spectral range of [1529.55, 1530.45] nm. We compute the area in Fig. 7(a) where $SNR_{recovered}/SNR_{target} > 0.1$, which accounts for only 0.48% of the total bandwidth search space. In this plot $SNR_{target} = 10$, resulting in *over 99.5% chance that the adversary is not able to have an SNR above 1*. Notice that this result is conservative since we assume the CFBG dispersion parameter to be fully matched.

B. CFBG Dispersion Parameter Matching

We next investigate the role dispersion effect plays in the stealth signal recovery. For the sake of simplicity, we assume $\lambda_{eav} = \lambda_{CFBG} = 1530$ nm and $\Delta\lambda_{eav} = \Delta\lambda_{Overlap}$, which is a strong assumption that allows the eavesdropper to guess the CFBG dispersion parameter within the 0.48% peak region of Fig. 7(a). Fig. 7(b) plots $SNR_{recovered}/SNR_{target}$ versus the eavesdropper's selection of $\Delta\lambda_{eav}$ and D_{eav}. In this plot,

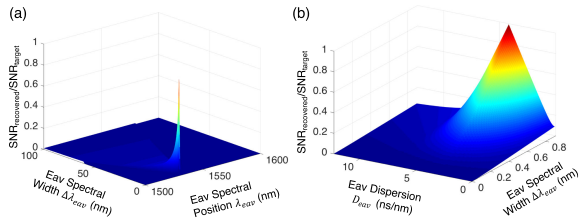

Fig. 7. Analysis of the stealth signal recovery effectiveness in terms of $SNR_{recovered}/SNR_{target}$ for the eavesdropper (a) who selects a pair of $\Delta\lambda_{eav} \in [0, 100]$ nm and $\lambda_{eav} \in [1500, 1600]$ nm when assuming $D_{eav} = D_{CFBG}$; (b) who selects a pair of $\Delta\lambda_{eav} \in [0, 0.9]$ nm and $D_{eav} \in [0, 12.3]$ ns/nm when assuming $\lambda_{eav} = \lambda_{CFBG} = 1530$ nm and $\Delta\lambda_{eav} = \Delta\lambda_{Overlap}$.

$\Delta\lambda_{CFBG} = 0.9$ nm while $D_{CFBG} = 4.1$ ns/nm. We consider the searching range for the CFBG dispersion parameter to be [0, 12.3] ns/nm. We also compute the area in Fig. 7(b) where $SNR_{recovered}/SNR_{target} > 0.1$, which accounts for 21.71% of the total key space considered here. We have to emphasize that this result is conservative by setting finite bounds on the dispersion parameters to be considered, and assuming the eavesdropper has successfully located the target ASE noise bandwidth position.

C. Summarizing Remarks

The total success rate for the eavesdropper to effectively match both the ASE noise bandwidth and CFBG dispersion parameter is about 2^{-10}. Given the fact that data is generally transmitted at a high rate over an optical channel, the eavesdropper has to recover the stealth signal right at the moment it is received. Therefore, in real-time, the eavesdropper literally has only one chance to match the system parameters used for generating the stealth signal. Without any prior knowledge, the eavesdropper has to randomly guess the system parameters. A searching algorithm for the system parameters takes time to run (especially using physical hardware), and can be easily counter-measured by employing standard cryptographic pseudo-random number generators (on both sides) and a pre-shared key/seed to update the system parameters for every single bit being transmitted.

VI. Security Against Stealth Signal Detection

In this section, we evaluate our steganographic communication system security against an eavesdropper who performs a statistical analysis of the signal observed from the transmission channel, aiming to identify any stealth signal hidden beneath. Such a threat model is generally considered by the steganography community, and can be more powerful than brute-forcing the system parameters as it requires only a copy of the transmission channel signal to compromise the steganographic communication even without recovering the stealth signal. We first model the stealth signal detection in the framework of a hypothesis testing problem, then present quantitative result that bounds the eavesdropper's ability to distinguish the stealth signal from the transmission channel, and finally corroborate our analysis via experimental validation that applies a machine learning classifier to the statistical features of the eavesdropped transmission channel signal.

A. Hypothesis Testing Problem

Hypothesis testing is a statistical test that is used to determine which one of the two potential hypothesis H_0 or H_1 is the true explanation for an observation q [48]. Suppose there are two plausible probability distributions, p_{q0} and p_{q1}, defined over the space Q of possible observations. If H_0 is true, then q is generated according to p_{q0}; if H_1 is true, then q is generated according to p_{q1}.

In this work, we frame the eavesdropper's adversarial goal of distinguishing the stealth signal from the transmission channel as a hypothesis testing problem. Recall our steganographic communication system where CFBG1 may select a small ASE noise bandwidth to be modulated with the stealth data while most of the ASE noise outside of the CFBG bandwidth remains as the *pure ASE noise* in the transmission channel. The sender then operates in one of two modes:

- In the first mode, the sender is inactive and has no stealth data modulated onto the selected ASE noise bandwidth. However, this particular pure ASE noise will still be spread by CFBG2 and become the *spread pure ASE noise*.
- In the second mode, the sender is active and does have stealth data modulated onto the selected ASE noise bandwidth. Such a data-carrying ASE noise will be spread by CFBG2 and become the *spread data-carrying ASE noise*.

The hypothesis testing problem faced by the eavesdropper, therefore, is to determine which one of the following two hypotheses is correct:

- Hypothesis H_0: It is the spread pure ASE noise that is embedded within the pure ASE noise in the transmission channel.
- Hypothesis H_1: It is the spread data-carrying ASE noise that is embedded within the pure ASE noise in the transmission channel.

B. Probability Distributions of Transmission Channel Signal

Fig. 8 illustrates various types of the ASE noise and their probability distributions. The top row shows the case where there is no stealth data modulated onto the ASE noise (selected by CFBG1), and the bottom row shows the case where there is stealth data modulated onto the ASE noise (selected by CFBG1). Suppose we deliver a single bit (either bit 0 or bit 1) over the steganographic channel. Since the pure ASE noise can be statistically described as a Gaussian distribution [49], the probability distribution of the data-carrying ASE noise is also a Gaussian distribution:

- The probability distribution of the pure ASE noise is $p_n(I) = N(\mu_n, \sigma_n^2)$ with mean μ_n and variance σ_n^2.
- The probability distribution of the data-carrying ASE noise is $p_d(I) = N(\mu_d, \sigma_d^2)$ with mean μ_d and variance σ_d^2.

The signal spreading (performed by CFBG2) does not change the total energy of a signal. Therefore, spreading the signal temporally will lead to a reduction in the signal power level, which is valid for both the spread pure ASE noise and spread data-carrying ASE noise (as shown in Fig. 8):

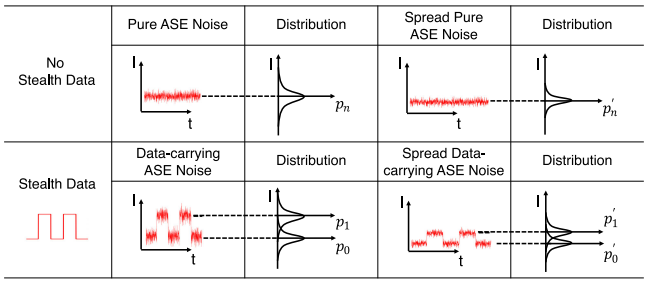

Fig. 8. Schematic illustrations of various types of the ASE noise and their probability distributions when the ASE noise carries no stealth data (top), or the ASE noise carries stealth data (bottom).

- The probability distribution of the spread pure ASE noise is $p_n'(I) = N(\mu_n', \sigma_n'^2)$ where μ_n' and $\sigma_n'^2$ are the corresponding post-spreading mean and variance.
- The probability distribution of the spread data-carrying ASE noise is $p_d'(I) = N(\mu_d', \sigma_d'^2)$ where μ_d' and $\sigma_d'^2$ are the corresponding post-spreading mean and variance.

In the transmission channel, the spread pure ASE noise and spread data-carrying ASE noise are embedded within the pure ASE noise in a way such that:

- The probability distribution of the pure ASE noise containing the spread pure ASE noise is $p_n''(I) = N(\mu_n'', \sigma_n''^2)$ where $\mu_n'' = \mu_n + \mu_n'$, $\sigma_n''^2 = \sigma_n^2 + \sigma_n'^2$.
- The probability distribution of the pure ASE noise containing the spread data-carrying ASE noise is $p_d''(I) = N(\mu_d'', \sigma_d''^2)$ where $\mu_d'' = \mu_n + \mu_d'$, $\sigma_d''^2 = \sigma_n^2 + \sigma_d'^2$.

For the sake of steganographic communication purpose, we tend to make the pure ASE noise (from the public channel) dominate in the transmission channel where its power σ_n^2 is much higher than that of either spread pure ASE noise $\sigma_n'^2$ or spread data-carrying ASE noise $\sigma_d'^2$. We achieve this in our implementation by keeping the stealth channel ASE noise bandwidth a small part of the overall ASE noise spectrum, i.e., 0.9 nm width centered around 1530 nm. In that case, the pure ASE noise outside of the stealth channel bandwidth carries approximately 93.6% of the total ASE noise power in the transmission channel (as mentioned in [50], the 10 nm ASE noise power around 1530 nm contributes 71% power of the entire ASE spectrum). We provide detailed definitions of the above probability distributions and their connections with the dispersion effect in Appendix D.

C. Stealth Signal Indistinguishability

We next define whether the eavesdropper succeeds in the hypothesis testing via *statistical indistinguishability* of two probability distributions [51]:

- Relative entropy (known as Kullback-Leibler divergence):

$$D(p_d''(I)||p_n''(I)) = \int_{-\infty}^{\infty} p_d''(I) \log \frac{p_d''(I)}{p_n''(I)} dI$$
$$= \log\left(\frac{\sigma_n''}{\sigma_d''}\right) + \frac{\sigma_d''^2 + (\mu_d'' - \mu_n'')^2}{2\sigma_n''^2} - \frac{1}{2}. \quad (1)$$

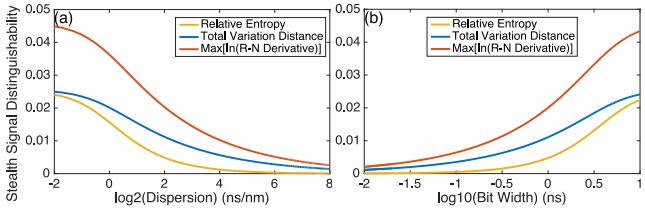

Fig. 9. The relative entropy, total variation distance, and maximum of logarithm of R-N derivative versus (a) the dispersion parameter, (b) the bit width. The (half of $1/e$-intensity) bit width in (a) is 1 ns; the dispersion parameter in (b) is 4.1 ns/nm.

- Total variation distance (L_1 norm):

$$V_T(p''_d(I), p''_n(I)) = \frac{1}{2}||p''_d(I) - p''_n(I)||_1 = \frac{1}{2\sqrt{2\pi}} \int_{-\infty}^{\infty} \left| \frac{1}{\sigma''_d} \exp\left[-\frac{(I-\mu''_d)^2}{2\sigma''^2_d}\right] - \frac{1}{\sigma''_n} \exp\left[-\frac{(I-\mu''_n)^2}{2\sigma''^2_n}\right] \right| dI. \quad (2)$$

- Logarithm of Radon-Nikodym (R-N) derivative:

$$\ln\left|\frac{dp''_d(I)}{dp''_n(I)}\right| = \ln\left|\frac{p''_d(I)}{p''_n(I)}\right| = \ln\left|\frac{\sigma''_n}{\sigma''_d} \exp\left[-\frac{(I-\mu''_d)^2}{2\sigma''^2_d} + \frac{(I-\mu''_n)^2}{2\sigma''^2_n}\right]\right|. \quad (3)$$

Formal information-theoretic models of steganography have adopted both the relative entropy [47], [52], and total variation distance [53], [54] to provide an *average* distinguishability for two probability distributions since Eq. (1) and (2) take every point on the probability distribution into considerations. We further embrace the logarithm of R-N derivative to characterize the distinguishability for two probability distributions from a differential privacy perspective [55], i.e., we may consider the *worst* privacy loss for the stealth signal by setting I to such value that results in the maximum of Eq. (3). Note that our work directly quantifies the eavesdropper's detectability of the steganographic communication as opposed to parallel works that quantified the stealth transmission capacity given eavesdropper's certain detectability of the steganographic communication [53], [56].

The steganographic communication system is said to be ϵ-*secure* provided that some small ϵ satisfying [47]

$$D(p''_d(I)||p''_n(I)) \leq \epsilon, V_T(p''_d(I), p''_n(I)) \leq \epsilon, \ln\left|\frac{dp''_d(I)}{dp''_n(I)}\right| \leq \epsilon. \quad (4)$$

$\epsilon = 0$ corresponds to the special case where the steganographic communication system is said to be *0-secure* if

$$D(p''_d(I)||p''_n(I)) = 0, V_T(p''_d(I), p''_n(I)) = 0, \ln\left|\frac{dp''_d(I)}{dp''_n(I)}\right| = 0. \quad (5)$$

In a 0-secure steganographic communication system, $p''_d(I)$ and $p''_n(I)$ share the same probability distribution so that the eavesdropper cannot distinguish whether there is a steganographic communication occurring in the transmission channel.

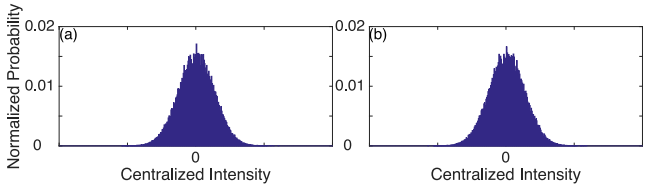

Fig. 10. Sample probability distribution of (a) the transmission channel signal containing the spread pure ASE noise, and (b) the transmission channel signal containing the data-carrying ASE noise.

We present the graphical relationship of the relative entropy, total variation distance, and maximum of logarithm of R-N derivative versus the dispersion parameter and (half of $1/e$-intensity) bit width in Fig. 9. As we increase the dispersion parameter or decrease the bit width (which is equivalent to higher bit rate), all these three curves (representing stealth signal distinguishability) reduce to 0. Given the same dispersion parameter (or bit width), the maximum of logarithm of R-N derivative is larger than the relative entropy and total variation distance. Therefore, the steganographic communication system is ϵ-*secure* if setting

$$\epsilon = \max_I \ln\left|\frac{\sigma''_n}{\sigma''_d} \exp\left[-\frac{(I-\mu''_d)^2}{2\sigma''^2_d} + \frac{(I-\mu''_n)^2}{2\sigma''^2_n}\right]\right|, \quad (6)$$

and approaches the 0-secure scenario if we are able to (a) apply a sufficiently large signal spreading to the data-carrying ASE noise, or (b) transmit the stealth data at a sufficiently high rate (see Appendix D for proof).

Our analytic results above show that *given certain conditions, the unique combination of the ASE noise and the signal spreading performed by CFBG enables the pure ASE noise containing the spread data-carrying ASE noise to be indistinguishable from the pure ASE noise containing the spread pure ASE noise.* We further extend our analysis to a multi-bit scenario in Appendix E to demonstrate the steganographic communication system is ϵ-*secure on average* against an eavesdropper who observes the probability distribution of more than a single bit.

D. Experimental Validation

Next, we will experimentally validate the stealth signal indistinguishability through machine learning techniques operating on real data collected from the experimental setup.

To emulate the eavesdropper who attempts to estimate the transmission channel signal probability distribution, we employ a Tektronix DSA8300 oscilloscope (containing a 20 GHz sampling unit) to sample the eavesdropped transmission channel signal. The "histogram" feature on the oscilloscope is used to estimate the sampled signal probability distribution. We collect 90 samples of the transmission channel signal containing the spread pure ASE noise (Fig. 10(a)) and 90 samples of the transmission channel signal containing the spread data-carrying ASE noise (Fig. 10(b)).

We build a machine learning classifier based on support vector machines (SVMs) to classify the estimated transmission channel

TABLE II
STEALTH SIGNAL CLASSIFICATIONS

Kernel Type	Linear Kernel		
Training/Testing Sample Size	60/120	90/90	120/60
Average Testing Error	49.91%	49.11%	48.67%
95% Confidence Interval	[0.41, 0.59]	[0.39, 0.59]	[0.36, 0.61]
Kernel Type	Gaussian Kernel		
Training/Testing Sample Size	60/120	90/90	120/60
Average Testing Error	50.91%	50.22%	50.33%
95% Confidence Interval	[0.42, 0.60]	[0.40, 0.61]	[0.38, 0.63]

signal probability distributions into one of two classes: transmission channel signal containing either the spread pure ASE noise or the spread data-carrying ASE noise. We divide samples of each class evenly to the training/testing set, and consider three partition ratios: 60/120, 90/90, 120/60 to balance the training set size effect. We choose both a linear kernel and a Gaussian kernel for the classifier. The features in this case are the 400 (bin) values of each probability distribution, which form a high dimensional feature space. We perform 10-fold cross-validation on the training set to select the parameters that minimize the training error before applying the classifier to the testing set.

We present the average testing error of our classifications in Table II, with the corresponding 95% confidence interval of each average testing error given as an indicator of how representative our results are:

- We first consider the classification results using the linear kernel. For the 60/120 partition ratio between the training and testing sets, the average testing error is 49.91% whose 95% confidence interval is [0.41, 0.59]. For the 90/90 partition ratio between the training and testing sets, the average testing error is 49.11% whose 95% confidence interval is [0.39, 0.59]. For the 120/60 partition ratio between the training and testing sets, the average testing error is 48.67% whose 95% confidence interval is [0.36, 0.61].
- We then consider the classification results using the Gaussian kernel. For the 60/120 partition ratio between the training and testing sets, the average testing error is 50.91% whose 95% confidence interval is [0.42, 0.60]. For the 90/90 partition ratio between the training and testing sets, the average testing error is 50.22% whose 95% confidence interval is [0.40, 0.61]. For the 120/60 partition ratio between the training and testing sets, the average testing error is 50.33% whose 95% confidence interval is [0.38, 0.63].

In general, the linear kernel performs slightly better than the Gaussian kernel (at such high dimensional feature space). The fact that the average testing errors are close to 50% suggests that *based on the observation of the transmission channel signal, the chance for the eavesdropper to correctly identify the stealth signal hidden in the transmission channel is equivalent to a random guess even with a finite dispersion parameter and data rate (such as those used in the prototype implementation).*

VII. CONCLUSIONS

We propose and demonstrate a steganographic communication technology that adopts a novel combination of the innate optical channel noise and a unique signal spreading function to prevent a link-level eavesdropper from detecting the stealth data being transmitted. We experimentally implement a prototype steganographic communication system that overlays a stealth communication channel upon the existing communication infrastructures with zero cover-signal overhead. Based on our prototype implementation, we perform (a) the frequency and time domain characterizations to validate that our scheme achieves the desired steganographic communication purpose; (b) the first practical long-distance (25–50 km) steganographic communication between real computers at the application layer (200–300 Mbps local file transfer rate and 25–30 Mbps Internet data rate); (c) the bit-error-rate measurements to show small channel interference when operating the public and stealth channels simultaneously. Our quantitative security evaluations further demonstrate that our approach (1) forces the eavesdropper to recover the stealth signal with a success rate of 2^{-10} by random guessing, and (2) strictly limits the eavesdropper's ability of detecting the stealth signal hidden in the transmission channel close to a random guess.

Our approach represents a new way of looking at communication security and privacy. In a conventional communication channel, an eavesdropper can see the data even without being able to compromise the encryption applied. In our scheme, it appears for the eavesdropper as if just noise in the transmission channel, which truly protects its users from giving away any of their information. Our technology can be applicable to many parts of today's communication infrastructure, including networks accessed by businesses and homes, the Internet backbone, and the wireless back-haul connecting cellular systems. It can be potentially important for communicating any data of high value, benefiting individuals and organizations ranging from private health-care and banking systems to sensitive data centers and government agencies.

Many potential extensions of this work exist. For example, our steganographic communication scheme opens the possibility for future multi-channel steganographic communications that can support much higher stealth data throughput using different sections of the entire ASE spectrum. We also expect a feasible steganographic communication protocol based on which two communicating parties can securely negotiate their system parameters.

APPENDIX A
DATA MODULATION/DEMODULATION

Given a modulating signal $m(t)$ and a carrier signal $c(t)$, the intensity modulator (IM) simply multiplies them together to output the modulated signal

$$f(t) = [1 + m(t)] \cdot c(t). \tag{7}$$

Ideally if there is no modulating signal or the modulating signal carries no power, i.e., $m(t) = 0$, the IM is transparent to the carrier signal $c(t)$.

When using a photo-detector (PD) to convert the optical signal to the electric signal:

$$P_{optical} = I_{electric}/R = AI_{electric}, \tag{8}$$

$$P_{electric} = R_L I^2_{electric} = BI^2_{electric}, \tag{9}$$

where R is the responsivity of the PD, R_L is the load resistance of the PD, $P_{optical}$ is the optical signal power, $P_{electric}$ is the electric signal power, and $I_{electric}$ is the electric signal intensity. When it comes to receiving the data-carrying ASE noise, the electric signal will behave in such a way that

$$I_{electric} = 2RS_{sp}\Delta\nu = C\Delta\nu \tag{10}$$

where S_{sp} is the spectral density of the ASE noise, and $\Delta\nu$ is the ASE noise bandwidth. Meanwhile, several types of electric noise will be induced, among which the following three dominate [57], [58]:

$$\sigma^2_{thermal} = 4k_BTF_n\Delta f/R_L = E, \tag{11}$$

$$\sigma^2_{beating} = 4R^2S^2_{sp}\Delta f\Delta\nu = F\Delta\nu, \tag{12}$$

$$\sigma^2_{shot} = 4qRS_{sp}\Delta f\Delta\nu = G\Delta\nu = HI_{electric}, \tag{13}$$

where k_B is Boltzmann constant, T is the room temperature, F_n is amplification ratio of the electric amplifier in PD, Δf is the electric bandwidth of the PD, and q is the electron charge. The thermal noise $\sigma^2_{thermal}$ accounts for the random thermal activities within a PD, the beating noise $\sigma^2_{beating}$ originates from the interference of two signals at slightly different frequencies within the ASE noise bandwidth, and the shot noise σ^2_{shot} results from the random generation of electrons within a PD whose strength is proportional to the electric signal intensity $I_{electric}$. These three types of electric noise generated at the PD ought not to be confused with the optical ASE noise existing in fiber-optic cables.

Appendix B
Dispersion Effect/Chirped Fiber Bragg Grating

The signal transmitted in optical communications typically consists of multiple frequency components (within the signal bandwidth). In an optical media, the transmission speed of each frequency component inherently differs from each other and leads to a temporal spreading of the signal after transmitting over a certain fiber distance. This phenomenon is called dispersion effect, which can be characterized by the dispersion parameter D (in the unit of ns/nm). From the perspective of a reliable signal transmission, the dispersion effect should be minimized and needs to be compensated before data demodulation. However, the dispersion effect can also be used to obscure the intensity modulated signals by lowering the signal power level close to or even below the noise floor, which serves as an enabler for the steganographic communication.

Instead of using the natural dispersion effect resulting from transmitting signals over a long-distance fiber, we intentionally introduce a stronger dispersion effect to the data-carrying ASE noise using a device called chirped fiber Bragg grating (CFBG) [59]. The CFBG inputs the optical signal on one side, reflects back the signal over a selected bandwidth (called the CFBG bandwidth), and outputs the signal not within the selected bandwidth on the other side. Such a bandwidth selection function is useful for spreading the reflected signal because the CFBG reflects different frequency components within its bandwidth at different times, which is equivalent to introducing a huge amount of time delay among frequency components. Being only 20 cm in length, the CFBG can achieve the same dispersion effect as an optical fiber hundreds of kilometers long [60]. Placing two CFBGs with the same bandwidth and dispersion parameter in the opposite orientations makes a perfect pair of signal stretcher and compressor.

Mathematically speaking, the dispersion effect is illustrated in the signal temporally spread by a *broadening factor* (BF) [61]:

$$BF = \sqrt{1 + 2\Big(D\Delta\lambda/\tau\Big)^2} \tag{14}$$

where D (in the unit of ns/nm) is the dispersion parameter of CFBG, $\Delta\lambda$ (in the unit of nm) is the ASE noise bandwidth used to carry the stealth data, and τ (in the unit of ns) is half of $1/e$-intensity bit width before signal spreading. While all these three parameters contribute to the dispersion effect, we tend to keep $\Delta\lambda$ a small part of the overall transmission channel ASE noise bandwidth in this work, and τ is subject to the electrical I/O speed of user's network interface card.

Note that the total signal energy remains the same even after being temporally spread. Hence, we have the product

$$P_{electric} \times (BF \cdot \tau) = \text{constant}. \tag{15}$$

Combining Eq. (9), (14), (15), we have

$$I_{spread} = I_{initial}/\sqrt{BF} \tag{16}$$

that relates the electric signal intensity after signal spreading I_{spread} to that before signal spreading $I_{initial}$ as a function of BF.

Appendix C
Stealth Signal Recovery Effectiveness

SNR_{target} is the stealth signal SNR achieved by the legitimate receiver in recovering the stealth signal after successfully matching $\Delta\nu_{CFBG}$ and D_{CFBG}. The signal and noise terms can both be written following Eq. (9), (10), (11), (12), (13) with the only modification that $\Delta\nu$ is replaced with $\Delta\nu_{CFBG}$:

$$SNR_{target} = \frac{BC^2\Delta\nu^2_{CFBG}}{E + (F+G)\Delta\nu_{CFBG}}. \tag{17}$$

$SNR_{recovered}$ is the recovered signal SNR achieved by the eavesdropper, i.e., $\Delta\nu_{CFBG}$ and D_{CFBG} are to be matched by $\Delta\nu_{eav}$ and D_{eav}. The noise term can be directly modified as

$$P_{noise} = E + (F+G)\Delta\nu_{eav} \tag{18}$$

while the signal term requires more thoughts. First, $\Delta\nu_{eav}$ can be either larger or smaller than $\Delta\nu_{CFBG}$. Second, only the part of $\Delta\nu_{eav}$ that falls within $\Delta\nu_{CFBG}$ contributes to the signal. Therefore, we define a new bandwidth parameter, $\Delta\nu_{Overlap}$, to represent the overlapping bandwidth between $\Delta\nu_{eav}$ and $\Delta\nu_{CFBG}$. We may now express the signal term as

$$P_{signal} = BC^2\Delta\nu^2_{Overlap}, \tag{19}$$

$$0 \leqslant \Delta\nu_{Overlap} \leqslant \min\{\Delta\nu_{eav}, \Delta\nu_{CFBG}\}. \tag{20}$$

Putting together Eq. (18), (19), we have

$$SNR_{recovered} = \frac{BC^2\Delta\nu_{Overlap}^2}{E + (F+G)\Delta\nu_{eav}}. \tag{21}$$

We also need to consider matching D_{CFBG} with D_{eav}. Based on Eq. (10) and (16), we introduce *dispersion recovery ratio (DRR)* that corresponds to one of the following *under-compensating*, *over-compensating*, and *extra-spreading* cases:

$$DRR = \frac{\sqrt{1 + \left(D_{eav}\Delta\lambda_{Overlap}/\tau\right)^2}}{\sqrt{1 + \left(D_{CFBG}\Delta\lambda_{CFBG}/\tau\right)^2}} \tag{22}$$

when $D_{eav} < D_{CFBG}$;

$$DRR = \frac{\sqrt{1 + \left[(2D_{CFBG} - D_{eav})\Delta\lambda_{Overlap}/\tau\right]^2}}{\sqrt{1 + \left(D_{CFBG}\Delta\lambda_{CFBG}/\tau\right)^2}} \tag{23}$$

when $D_{CFBG} < D_{eav} < 2D_{CFBG}$;

$$DRR = \frac{1}{\sqrt{1 + \left[(-D_{CFBG} + D_{eav})\Delta\lambda_{CFBG}/\tau\right]^2}} \tag{24}$$

when $D_{eav} > 2D_{CFBG}$. In the above equations, $\Delta\lambda_{Overlap}$ is the overlapping spectral width (in the unit of nm), $\Delta\lambda_{CFBG}$ is the target CFBG spectral width (in the unit of nm).

Therefore, we may eventually write down the stealth signal recovery effectiveness as

$$\frac{SNR_{recovered}}{SNR_{target}} = \frac{\Delta\nu_{Overlap}^2/(C_1 + C_2\Delta\nu_{eav})}{\Delta\nu_{CFBG}^2/(C_1 + C_2\Delta\nu_{CFBG})} DRR \tag{25}$$

where $C_1 = E$ and $C_2 = F + G$. The above result is valid for the case where there is stealth data being transmitted. When there is no stealth data, the stealth signal power is equal to zero, leading to $SNR_{target} = 0$ and $SNR_{recovered} = 0$ no matter what $\Delta\nu_{eav}$ and D_{eav} are selected by the eavesdropper.

Appendix D
Stealth Signal Probability Distributions

The pure ASE noise can be statistically described as a Gaussian distribution $p_n(I)$ with mean μ_n and variance σ_n^2 [49]:

$$p_n(I) = \frac{1}{\sqrt{2\pi}\sigma_n}\exp\left[-\frac{(I-\mu_n)^2}{2\sigma_n^2}\right]. \tag{26}$$

As the stealth data (either bit 0 or bit 1) is modulated onto the ASE noise (selected by CFBG1), the probability distribution of the data-carrying ASE is also a Gaussian distribution $p_d(I)$ with mean μ_d and variance σ_d^2:

$$p_d(I) = \frac{1}{\sqrt{2\pi}\sigma_d}\exp\left[-\frac{(I-\mu_d)^2}{2\sigma_d^2}\right]. \tag{27}$$

It is worth mentioning that (a) μ_n is the noise floor of the pure ASE noise while μ_d depends on the modulating signal power; (b) σ_n^2 and σ_d^2 are differed by the shot noise σ_{shot}^2 that is proportional to the optical power of the received signal (recall Eq. (8), (13)):

$$\sigma^2 = \sigma_{thermal}^2 + \sigma_{beating}^2 + \sigma_{shot}^2. \tag{28}$$

The signal spreading (performed by CFBG2) will lead to a reduction in the signal power level. This is valid for both the spread pure ASE noise and spread data-carrying ASE noise whose probability distributions should be modified accordingly using Eq. (11), (12), (13), (16), (28). The probability distribution of the spread pure ASE noise is

$$p_n'(I) = \frac{1}{\sqrt{2\pi}\sigma_n'}\exp\left[-\frac{(I-\mu_n')^2}{2\sigma_n'^2}\right] \tag{29}$$

where μ_n' and $\sigma_n'^2$ are the corresponding post-spreading mean and variance:

$$\mu_n' = \mu_n/\sqrt{BF}, \tag{30}$$

$$\sigma_n'^2 = E + F\Delta\nu + H\mu_n'. \tag{31}$$

The probability distribution of the spread data-carrying ASE noise is

$$p_d'(I) = \frac{1}{\sqrt{2\pi}\sigma_d'}\exp\left[-\frac{(I-\mu_d')^2}{2\sigma_d'^2}\right] \tag{32}$$

where μ_d' and $\sigma_d'^2$ are the corresponding post-spreading mean and variance:

$$\mu_d' = \mu_d/\sqrt{BF}, \tag{33}$$

$$\sigma_d'^2 = E + F\Delta\nu + H\mu_d'. \tag{34}$$

We may then write the probability distribution of the pure ASE noise containing the spread pure ASE noise as

$$p_n''(I) = \frac{1}{\sqrt{2\pi}\sigma_n''}\exp\left[-\frac{(I-\mu_n'')^2}{2\sigma_n''^2}\right] \tag{35}$$

where $\mu_n'' = \mu_n + \mu_n'$ and $\sigma_n''^2 = \sigma_n^2 + \sigma_n'^2$ are the corresponding mean and variance. Similarly, the probability distribution of the pure ASE noise containing the spread data-carrying ASE noise is

$$p_d''(I) = \frac{1}{\sqrt{2\pi}\sigma_d''}\exp\left[-\frac{(I-\mu_d'')^2}{2\sigma_d''^2}\right] \tag{36}$$

where $\mu_d'' = \mu_n + \mu_d'$ and $\sigma_d''^2 = \sigma_n^2 + \sigma_d'^2$ are the corresponding mean and variance.

One straightforward conclusion from the above equations is as $D \to \infty$ (or $\tau \to 0$), $BF \to \infty$, and $\mu_d' \to \mu_n'$, $\sigma_d'^2 \to \sigma_n'^2$, and eventually $\mu_d'' \to \mu_n''$, $\sigma_d''^2 \to \sigma_n''^2$. In consequence, $p_d'(I)$ moves closer to $p_n'(I)$ with a sufficiently large signal spreading or a sufficiently high data rate.

Appendix E
Multi-Bit Stealth Signal Indistinguishability

Our theoretical analysis in section VI quantifies the stealth signal indistinguishability of transmitting a single bit over the transmission channel. We now extend our analysis to a multi-bit scenario where the eavesdropper may observe the probability distribution of n bits. We may further approximate the continuous information embedding process as a (stochastic)

Gaussian process such that for any choice of distinct values of $\{t_1, ..., t_n \in T\}$ where T is the observation period, the corresponding signal observation of $\boldsymbol{I} = \{I_{t1}, ..., I_{tn}\}$ has a multivariate Gaussian distribution with mean vector $\boldsymbol{\mu}$ and covariance matrix $\boldsymbol{\Sigma}$:

$$p(\boldsymbol{I}) = \frac{1}{(2\pi)^{n/2} det(\boldsymbol{\Sigma})^{1/2}} \exp\Big[-\frac{1}{2}(\boldsymbol{I}-\boldsymbol{\mu})^T \boldsymbol{\Sigma}^{-1}(\boldsymbol{I}-\boldsymbol{\mu})\Big]. \tag{37}$$

Different sequence of bit 0 s and 1 s observed will lead to different mean vector $\boldsymbol{\mu}$ and covariance matrix $\boldsymbol{\Sigma}$. Ideally, the bit 0 of the stealth data carries no power, which is equivalent to the case where there is no stealth data for modulation. Hence, the bit 0 carried by the ASE noise is identical to the pure ASE noise at the same bandwidth. Consider the best case for the eavesdropper where a sequence of all 0 s (or equivalently transmitting no stealth data) and a sequence of all 1 s are observed, which is supposed to result in the largest stealth signal distinguishability. We denote p^n_{q0} for the multivariate probability distribution of the transmission channel signal containing a sequence of all spread 0 s, and p^n_{q1} for the multivariate probability distribution of the transmission channel signal containing a sequence of all spread 1 s. Their corresponding mean vectors and covariance matrices are $\boldsymbol{\mu}^n_0$, $\boldsymbol{\Sigma}^n_0$ and $\boldsymbol{\mu}^n_1$, $\boldsymbol{\Sigma}^n_1$, respectively. Assuming independently repeated observations of the transmission channel signal, covariance matrices $\boldsymbol{\Sigma}^n_0$ and $\boldsymbol{\Sigma}^n_1$ are diagonal.

We adopt the same definition in [47], and extend it so that the steganographic communication system is said to be *ϵ-secure on average* if there exists some small ϵ satisfying

$$\lim_{n\to\infty} \frac{1}{n} D(p^n_{q0}||p^n_{q1}) \le \epsilon, \tag{38}$$

$$\lim_{n\to\infty} \frac{1}{n} V_T(p^n_{q0}, p^n_{q1}) \le \epsilon, \tag{39}$$

$$\lim_{n\to\infty} \frac{1}{n}\Big(\ln\Big|\frac{dp^n_{q0}}{dp^n_{q1}}\Big|\Big) \le \epsilon. \tag{40}$$

Considering that the relative entropy follows the chain rule $D(p^n_{q0}||p^n_{q1}) = nD(p_{q0}||p_{q1})$ and the total variation distance uses L_1 norm, Eq. (38), (39) will hold as long as their corresponding one-bit scenario holds. As for the R-N derivative between p^n_{q0} and p^n_{q1}:

$$\begin{aligned}\frac{dp^n_{q1}}{dp^n_{q0}} &= \frac{det(\boldsymbol{\Sigma}^n_0)^{-1/2}}{det(\boldsymbol{\Sigma}^n_1)^{-1/2}} \exp\Big[-\frac{1}{2}(\boldsymbol{I}-\boldsymbol{\mu}^n_1)^T(\Sigma^n_1)^{-1}(\boldsymbol{I}-\boldsymbol{\mu}^n_1) \\ &\quad + \frac{1}{2}(\boldsymbol{I}-\boldsymbol{\mu}^n_0)^T(\Sigma^n_0)^{-1}(\boldsymbol{I}-\boldsymbol{\mu}^n_0)\Big] \\ &= \left(\frac{\sigma''_0}{\sigma''_1}\right)^n \exp\left[-\frac{n^2(I-\mu''_1)^2}{2n(\sigma''_1)^2} + \frac{n^2(I-\mu''_0)^2}{2n(\sigma''_0)^2}\right].\end{aligned} \tag{41}$$

Therefore, we can still set

$$\begin{aligned}\epsilon &= \max_I \lim_{n\to\infty} \frac{1}{n}\ln\Big|\frac{dp^n_{q1}}{dp^n_{q0}}\Big| \\ &= \max_I \ln\left|\frac{\sigma''_0}{\sigma''_1}\exp\left[-\frac{(I-I''_1)^2}{2\sigma''^2_1} + \frac{(I-I''_0)^2}{2\sigma''^2_0}\right]\right|\end{aligned} \tag{42}$$

which is the same upper bound as Eq. (6). The steganographic communication system also approaches *0-secure on average* if applying a sufficiently large signal spreading or transmitting the stealth data at a sufficiently high rate.

REFERENCES

[1] V. Gurung, "Kevin mitnick hack fiber optic and steal sensitive data," Jun. 2015. [Online]. Available: https://www.cyberkendra.com/2015/06/kevin-mitnick-hack-fiber-optic-and.html

[2] J. Ruppe, "Fiber optic tapping—Tapping setup," Oct. 2015. [Online]. Available: https://www.joshruppe.com/fiber-optic-tapping-tapping-setup/

[3] Y. Grauer, "Security news this week: Someone's cutting fiber optic cables in the bay area," Nov. 2015. [Online]. Available: https://www.wired.com/2015/11/security-news-this-week-bay-area-fiber-optic-cables-mysteriously-cut/

[4] S. Moss, "World's largest internet exchange sues German spy agency for tapping data center," May 2018. [Online]. Available: http://www.datacenterdynamics.com/content-tracks/security-risk/worlds-largest-internet-exchange-sues-german-spy-agency-for-tapping-data-center/100204.fullarticle/

[5] K. Zetter, "U.K. spy agency secretly taps over 200 fiber-optic cables, shares data with the NSA," Jun. 2013. [Online]. Available: https://www.wired.com/2013/06/gchq-tapped-200-cables/

[6] O. Khazan, "The creepy, long-standing practice of undersea cable tapping," Jul. 2016. [Online]. Available: http://www.theatlantic.com/international/archive/2013/07/the-creepy-long-standing-practice-of-undersea-cable-tapping/277855/

[7] E. MacAskill, J. Borger, N. Hopkins, N. Davies, and J. Ball, "GCHQ taps fibre-optic cables for secret access to world's communications," Jun. 2013. [Online]. Available: http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa

[8] J. Ball, "NSA stores metadata of millions of web users for up to a year, secret files show," Sep. 2013. [Online]. Available: http://www.theguardian.com/world/2013/sep/30/nsa-americans-metadata-year-documents

[9] J.-F. Raymond, "Traffic analysis: Protocols, attacks, design issues, and open problems," in *Proc. Int. Workshop Design. Privacy Enhancing Technol., Design Issues Anonymity Unobservability*, 2001, pp. 10–29.

[10] A. Back, U. Möller, and A. Stiglic, "Traffic analysis attacks and trade-offs in anonymity providing systems," in *Proc. Int. Workshop Inf. Hiding*, 2001, pp. 245–257.

[11] N. Mathewson and R. Dingledine, "Practical traffic analysis: Extending and resisting statistical disclosure," in *Proc. Int. Workshop Privacy Enhancing Technol.*, 2004, pp. 17–34.

[12] S. J. Murdoch and G. Danezis, "Low-cost traffic analysis of tor," in *Proc. IEEE Symp. Secur. Privacy*, 2005, pp. 183–195.

[13] E. W. Felten and M. A. Schneider, "Timing attacks on web privacy," in *Proc. 7th ACM Conf. Comput. Commun. Secur.*, 2000, pp. 25–32. [Online]. Available: http://doi.acm.org/10.1145/352600.352606

[14] X. Gong, N. Borisov, N. Kiyavash, and N. Schear, "Website detection using remote traffic analysis," in *Proc. Int. Symp. Privacy Enhancing Technol. Symp.*, 2012, pp. 58–78.

[15] T. Wang, X. Cai, R. Nithyanand, R. Johnson, and I. Goldberg, "Effective attacks and provable defenses for website fingerprinting," in *Proc. 23rd USENIX Secur. Symp.*, 2014, pp. 143–157.

[16] S. M. Bellovin, "A technique for counting natted hosts," in *Proc. 2nd ACM SIGCOMM Workshop Internet Measurement*, 2002, pp. 267–272. [Online]. Available: http://doi.acm.org/10.1145/637201.637243

[17] T. Kohno, A. Broido, and K. C. Claffy, "Remote physical device fingerprinting," *IEEE Trans. Dependable Secure Comput.*, vol. 2, no. 2, pp. 93–108, Apr. 2005.

[18] R. A. Scholtz, "The origins of spread-spectrum communications," *IEEE Trans. Commun.*, vol. 30-C, no. 5, pp. 822–854, May 1982.

[19] R. L. Pickholtz, D. L. Schilling, and L. B. Milstein, "Theory of spread-spectrum communications–A tutorial," *IEEE Trans. Commun.*, vol. 30, no. 5, pp. 855–884, May 1982.

[20] A. J. Viterbi, "Spread spectrum communications: Myths and realities," *IEEE Commun. Mag.*, vol. 40, no. 5, pp. 34–41, May 2002.

[21] D. L. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms," *Commun. ACM*, vol. 24, no. 2, pp. 84–90, Feb. 1981. [Online]. Available: http://doi.acm.org/10.1145/358549.358563

[22] R. Dingledine, N. Mathewson, and P. Syverson, "Tor: The second-generation onion router," in *Proc. 13th Conf. USENIX Secur. Symp.*, 2004, pp. 21–21. [Online]. Available: http://dl.acm.org/citation.cfm?id=1251375.1251396

[23] J. Jrandom, "I2p anonymous network: Technical introduction," Dec. 13, 2010. [Online]. Available: https://geti2p.net/en/docs/how/tech-intro
[24] L. Boney, A. H. Tewfik, and K. N. Hamdy, "Digital watermarks for audio signals," in *Proc. 3rd IEEE Int. Conf. Multimedia Comput. Syst.*, Jun. 1996, pp. 473–480.
[25] C.-T. Hsu and J.-L. Wu, "Hidden digital watermarks in images," *IEEE Trans. Image Process.*, vol. 8, no. 1, pp. 58–68, Jan. 1999.
[26] R. G. van Schyndel, A. Z. Tirkel, and C. F. Osborne, "A digital watermark," in *Proc. IEEE Int. Conf. Image Process.*, Nov. 1994, vol. 2, pp. 86–90.
[27] R. B. Wolfgang and E. J. Delp, "A watermark for digital images," in *Proc. Int. Conf. Image Process.*, Sep. 1996, vol. 3, pp. 219–222.
[28] R. J. Anderson and F. A. Petitcolas, "On the limits of steganography," *IEEE J. Sel. Areas Commun.*, vol. 16, no. 4, pp. 474–481, May 1998.
[29] W. Bender, D. Gruhl, N. Morimoto, and A. Lu, "Techniques for data hiding," *IBM Syst. J.*, vol. 35, no. 3.4, pp. 313–336, 1996.
[30] N. F. Johnson and S. Jajodia, "Exploring steganography: Seeing the unseen," *Computer*, vol. 31, no. 2, pp. 26–34, 1998.
[31] D. Artz, "Digital steganography: Hiding data within data," *IEEE Internet Comput.*, vol. 5, no. 3, pp. 75–80, May/Jun. 2001.
[32] K. Ahsan and D. Kundur, "Practical data hiding in TCP/IP," in *Proc. Workshop Multimedia Secur. ACM Multimedia*, vol. 2, no. 7, pp. 7–19, 2002.
[33] S. Cabuk, C. E. Brodley, and C. Shields, "IP covert timing channels: Design and detection," in *Proc. 11th ACM Conf. Comput. Commun. Secur.*, 2004, pp. 178–187.
[34] S. J. Murdoch and S. Lewis, "Embedding covert channels into TCP/IP," in *Proc. Int. Workshop Inf. Hiding*, 2005, pp. 247–261.
[35] H. Wang and S. Wang, "Cyber warfare: Steganography vs. steganalysis," *Commun. ACM*, vol. 47, no. 10, pp. 76–82, 2004.
[36] B. B. Wu and E. E. Narimanov, "A method for secure communications over a public fiber-optical network," *Opt. Express*, vol. 14, no. 9, pp. 3738–3751, 2006.
[37] Y. Huang, B. Wu, I. Glesk, E. Narimanov, T. Wang, and P. Prucnal, "Combining cryptographic and steganographic security with self-wrapped optical code division multiplexing techniques," *Electron. Lett.*, vol. 43, no. 25, pp. 1449–1451, 2007.
[38] K. Kravtsov, B. Wu, I. Glysk, P. Prucnal, and E. Narimanov, "Stealth transmission over a WDM network with detection based on an all-optical thresholder," in *Proc. IEEE Lasers Electro-Optics Soc. Annu. Meeting Conf.*, 2007, pp. 480–481.
[39] X. Hong, D. Wang, L. Xu, and S. He, "Demonstration of optical steganography transmission using temporal phase coded optical signals with spectral notch filtering," *Opt. Express*, vol. 18, no. 12, pp. 12 415–12 420, 2010.
[40] 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.
[41] Z. Gao, X. Wang, N. Kataoka, and N. Wada, "Stealth transmission of time-domain spectral phase encoded OCDMA signal over WDM network," *IEEE Photon. Technol. Lett.*, vol. 22, no. 13, pp. 993–995, Jul. 2010.
[42] M. P. Fok and P. R. Prucnal, "Compact and low-latency scheme for optical steganography using chirped fibre Bragg gratings," *Electron. Lett.*, vol. 45, no. 3, pp. 179–180, 2009.
[43] B. Wu *et al.*, "Optical steganography based on amplified spontaneous emission noise," *Opt. Express*, vol. 21, no. 2, pp. 2065–2071, 2013.
[44] 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, 2014.
[45] 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, 2014.
[46] P. Y. Ma, B. Wu, B. J. Shastri, and P. R. Prucnal, "Optical steganography communication using signal-carrying noise dispersion," in *Proc. IEEE Photon. Conf.*, Oct. 2016, pp. 55–56.
[47] C. Cachin, "An information-theoretic model for steganography," *Inf. Comput.*, vol. 192, no. 1, pp. 41–56, 2004.
[48] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. Hoboken, NJ, USA: Wiley, 2012.
[49] P. A. Govind, *Fiber-Optic Communication Systems.* Hoboken, NJ, USA: Wiley, 2002.
[50] 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.
[51] P. Cuff and L. Yu, "Differential privacy as a mutual information constraint," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, 2016, pp. 43–54.
[52] J. Hou and G. Kramer, "Effective secrecy: Reliability, confusion and stealth," in *Proc. IEEE Int. Symp. Inf. Theory*, Jun. 2014, pp. 601–605.
[53] B. A. Bash, D. Goeckel, and D. Towsley, "Limits of reliable communication with low probability of detection on AWGN channels," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1921–1930, Sep. 2013.
[54] P. H. Che, M. Bakshi, and S. Jaggi, "Reliable deniable communication: Hiding messages in noise," in *Proc. IEEE Int. Symp. Inf. Theory*, Jul. 2013, pp. 2945–2949.
[55] C. Dwork and G. N. Rothblum, "Concentrated differential privacy," *CoRR*, abs/1603.01887, 2016.
[56] B. A. Bash, D. Goeckel, and D. Towsley, "Square root law for communication with low probability of detection on AWGN channels," in *Proc. IEEE Int. Symp. Inf. Theory Proc.*, Jul. 2012, pp. 448–452.
[57] N. A. Olsson, "Lightwave systems with optical amplifiers," *J. Lightw. Technol.*, vol. 7, no. 7, pp. 1071–1082, Jul. 1989.
[58] R. Steele, G. Walker, and N. Walker, "Sensitivity of optically preamplified receivers with optical filtering," *IEEE Photon. Technol. Lett.*, vol. 3, no. 6, pp. 545–547, Jun. 1991.
[59] F. Ouellette, "Dispersion cancellation using linearly chirped Bragg grating filters in optical waveguides," *Opt. Lett.*, vol. 12, no. 10, pp. 847–849, 1987.
[60] P. Krug, T. Stephens, G. Yoffe, F. Ouellette, P. Hill, and G. Dhosi, "Dispersion compensation over 270 km at 10 gbit/s using an offset-core chirped fibre Bragg grating," *Electron. Lett.*, vol. 31, no. 13, pp. 1091–1093, 1995.
[61] D. Marcuse, "Pulse distortion in single-mode fibers. 3: Chirped pulses," *Appl. Opt.*, vol. 20, no. 20, pp. 3573–3579, 1981.

Philip Y. Ma received the B.S. degree in physics from Shanghai Jiao Tong University, Shanghai, China, in 2014, and the M.A. degree in electrical engineering from Princeton University, Princeton, NJ, USA, in 2016, where he is currently working toward the Ph.D. degree. His current research interests include optical signal processing, integrated photonic devices, physical layer security, and communication privacy.

Ben Wu received the B.Sc. (with distinction) degree from the Department of Optoelectronics, Nankai University, Tianjin, China, in 2008 and the Ph.D. (Hons.) degree from the Department of Electrical and Engineering, Princeton University, Princeton, NJ, USA. He is currently an Assistant Professor with the Department of Electrical and Computer Engineering, Rowan University. His research interests include optical stealth transmission, photonic signal processing, and optical imaging for health applications. He has the following awards: 2018 Health Hack Award by Inspira Health Network, 2014 Wu Prize for Excellence in Princeton University, 2013 Excellence in Teaching, 2009 Graduate Student Fellowship, and 2008 Excellent Graduation Thesis (top one out of 60 students).

Bhavin J. Shastri received the B.Eng (Hons. with distinction), M.Eng., and Ph.D. degrees in electrical engineering (photonics) from McGill University, Montreal, QC, Canada, in 2005, 2007, and 2012, respectively. He is currently an Assistant Professor of engineering physics with Queens University, Kingston, ON, Canada. He was an Associate Research Scholar (2016–2018) and a Banting and NSERC Postdoctoral Fellow (2012–2016) with Princeton University, USA. His research interests include silicon photonics, nanophotonics, photonic integrated circuits, and neuromophic computing with emphasis on applications such as information processing, nonlinear programming, and study of complex dynamical systems. He is a co-author of the book *Neuromorphic Photonics* (Taylor & Francis, CRC Press). He is a recipient of the 2014 Banting Postdoctoral Fellowship from the Government of Canada, the 2012 D. W. Ambridge Prize for the top graduating Ph.D. student, an IEEE Photonics Society 2011 Graduate Student Fellowship, a 2011 NSERC Postdoctoral Fellowship, a 2011 SPIE Scholarship in Optics and Photonics, a 2008 NSERC Alexander Graham Bell Canada Graduate Scholarship, and a 2007 Lorne Trottier Engineering Graduate Fellowship. He was the recipient of the Best Student Paper Awards at the 2010 IEEE Midwest Symposium on Circuits and Systems, the 2004 IEEE Computer Society Lance Stafford Larson Outstanding Student Award, and the 2003 IEEE Canada Life Member Award.

Alexander N. Tait received the Ph.D. degree from Professor Paul Prucnal in the Lightwave Communications Research Laboratory Group, Department of Electrical Engineering, Princeton University, Princeton, NJ, USA. He is a NRC Postdoctoral Fellow in the Quantum Nanophotonics and Faint Photonics Group, National Institute of Standards and Technology, Boulder, CO, USA. His research interests include silicon photonics, neuromorphic engineering, and superconducting optoelectronics. He is a recipient of the National Science Foundation Graduate Research Fellowship and is a member of the IEEE Photonics Society and the Optical Society of America. He is the recipient of the Award for Excellence from the Princeton School of Engineering and Applied Science, the Optical Engineering Award of Excellence from the Princeton Department of Electrical Engineering, the Best Student Paper Award at the 2016 IEEE Summer Topicals Meeting Series, and the Class of 1883 Writing Prize from the Princeton Department of English. He has authored 9 refereed papers and a book chapter, presented research at 13 technical conferences, and contributed to the textbook *Neuromorphic Photonics*.

Prateek Mittal is an Assistant Professor with Princeton University, Princeton, NJ, USA, where he is also with the Center for Information Technology Policy. His research aims to design and develop privacy preserving systems. A unifying theme in his work is to manipulate and exploit structural properties of networked systems to solve privacy challenges facing our society. His research has applied this distinct approach to widely used operational systems, and has used the resulting insights to influence system design and operation (including that of the Tor network and the Lets Encrypt certificate authority). He is the recipient of faculty research awards from IBM (2017), Intel (2016, 2017, 2018), Google (2016, 2017), Cisco (2016), the NSF CAREER Award (2016), the ONR YIP Award (2018), the ARO YIP Award (2018), Princeton University's E. Lawrence Keyes, Jr., Award for outstanding research and teaching (2017), and Princeton Innovation Award (2015, 2017, 2018). He has received several outstanding paper awards, including at ACM CCS, and has been named on the Princeton Engineering Commendation List for Outstanding Teaching four times. He serves on the editorial board of the Privacy Enhancing Technologies Symposium, and has co-chaired the workshops on Free and Open Communications on the Internet and Hot Topics in Privacy Enhancing Technologies.

Paul R. Prucnal (F'92) received the A.B. (*summa cum laude*) degree in mathematics and physics from Bowdoin College, Brunswick, ME, USA, and the M.S., M.Phil., and Ph.D. degrees in electrical engineering from Columbia University, New York, NY, USA. After the doctorate degree, he joined as a member of the faculty with Columbia University, where, as a member of the Columbia Radiation Laboratory, he performed groundbreaking work in OCDMA and self-routed photonic switching. In 1988, he joined as a member of the faculty with Princeton University. His research on optical CDMA initiated a new research field in which more than 1000 papers have been published, exploring applications ranging from information security to communication speed and bandwidth. In 1993, he invented the "Terahertz Optical Asymmetric Demultiplexer," the first optical switch capable of processing terabit per second (Tb/s) pulse trains. He has authored a book *Neuromorphic Photonics* (CRC Press, 2017), and was the Editor of the book *Optical Code Division Multiple Access: Fundamentals and Applications* (CRC Press, 2005). He has authored or coauthored more than 350 journal articles and book chapters and holds 28 U.S. patents. He was an Area Editor for the IEEE TRANSACTIONS ON COMMUNICATIONS. He is a Fellow of the Optical Society of America and the National Academy of Inventors, and a member of honor societies including Phi Beta Kappa and Sigma Xi. He was the recipient of the 1990 Rudolf Kingslake Medal for his paper entitled "Self-routing photonic switching with optically-processed control," received the Gold Medal from the Faculty of Mathematics, Physics, and Informatics, Comenius University, for leadership in the field of Optics 2006 and has won multiple teaching awards at Princeton, including the E-Council Lifetime Achievement Award for Excellence in Teaching, the School of Engineering and Applied Science Distinguished Teacher Award, and the President's Award for Distinguished Teaching. He has been instrumental in founding the field of neuromorphic photonics and developing the "photonic neuron," a high speed optical computing device modeled on neural networks, and integrated optical circuits to improve wireless signal quality by canceling radio interference.