Optical Signal Processing aq .I bandwid
hide the signal in plain sight. Because an eavesdrop
read the data nor detect the existence of the tran
optical stealth transmission provid es a higher l
hybrid system which includes both the public chan
channels can effectively provide anonymous co
defend against traffic analys is.

***Index Terms*—Optical encryption, key dist
neurons, optical steganography, amplified spo
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

data as the noise-like signa ls, 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,

Manuscript received October 21, 2014; revised March 16, 2015; accepted March 27, 2015. Date of pua eat http://ieeexplore.ieee.org.

Digital Object @ ebmitted

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

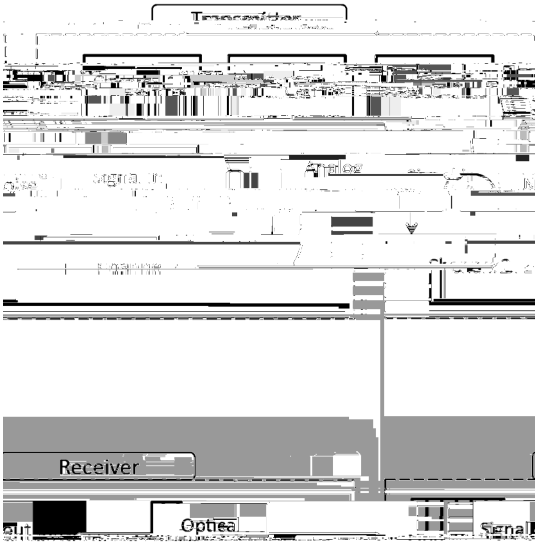

Fig. 2. Schematic diagram of analog noise encryption system.

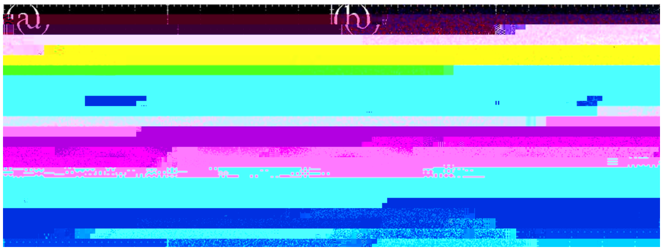

Fig. 3. (a) Eye diagrams of the encrypted signals with the interference can-

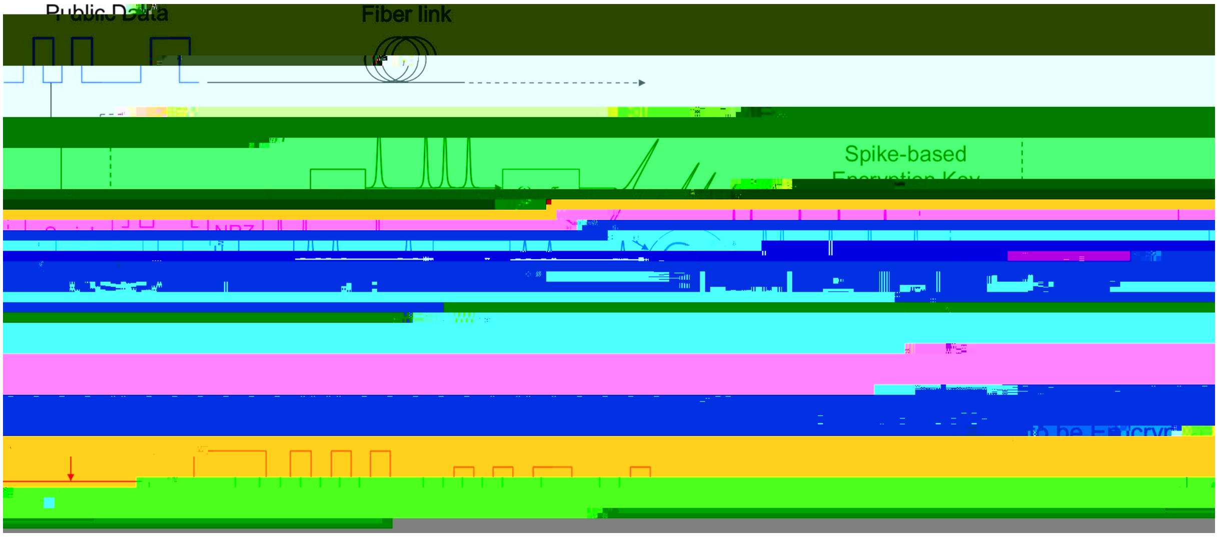

Fig. 5. Schematic diagram of key generation based on neuromorphic spike processing.

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 am

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

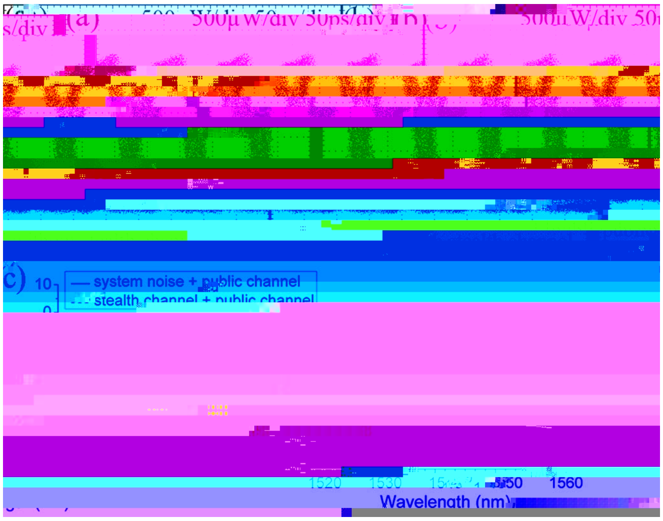

Fig. 9. (a) Eye diagram of public channel without stealth channel (b) Eye diagram of public channel with stealth channel (c) Spectrum of public channel with and without stealth channel. This figure is from [60].

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

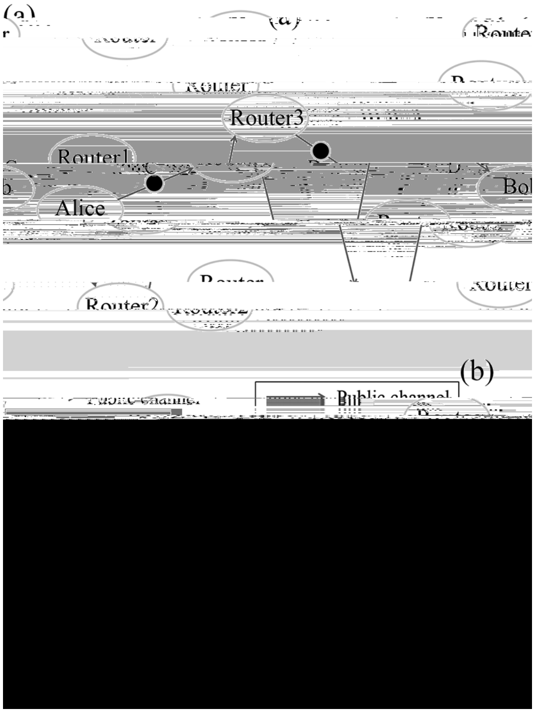

Fig. 10. Comparison of traditional Tor and Steganography assisted Tor (SAT).

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 and pure noise with either temporal or spectral domain analysis. In this way, optical stealth

[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.*

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