Photonic Layer Encryption in High Speed Optical Communications

Dan Sadot,[1,2,*] Eyal Wohlgemuth,[2] Ido Attia,[1,2] Ohad Balasiano,[1,2] Isaak Jonas,[1,2] Elimelech Keller,[2] and Hamutal Shalom[2]

[1] *Ben-Gurion University of the Negev, Be'er-Sheva, Israel.*
[2] *CyberRidge Ltd. Azrieli Sarona Tower. 121 Menachem Begin Rd. Tel-Aviv.*
[*] *dan.sadot@cyber-ridge.com*

Abstract: Combining multi-THz optical spectrum spreading, photonic phase encoding, and negative optical signal-to-noise ratio (OSNR) transmission, forms photonic shield that prevents data recording for offline deciphering. This supports post-quantum security by eliminating raw data availability for quantum computers processing.

1. Introduction

The demand for information confidentiality and security grows dramatically, particularly in light of the new era of quantum computing. Furthermore, sensitive applications, such as of military, governmental, financial, and healthcare sectors, are being increasingly exposed to cyber-attacks [1]. Existing digital encryption protocols are recently being perceived as limited and insufficient, and new generation of post-quantum cryptography (PQC) algorithms are being developed. Side by side, there is an increasing trend of adding a lower layer of protection, i.e. physical layer security (PLS). Several PLS approaches have been recently developed and are mentioned here. Quantum key distribution (QKD) [2] is considered unconditionally secured, i.e. completely resilient against cryptanalytic attacks. However, its performance is incomparable with the payload data rates, thus limited to key exchange only, while the payload encryption remains digital. In chaos-based communications [3], the user message is transmitted using a chaotic signal carrier, which is very sensitive to initial hardware conditions. All-optical processing techniques, such as optical XOR gates, have also been suggested. Recently, Y00 encryption schemes were demonstrated [4], based on extremely high-order random phase modulation using a pre-shared short key. The gap between the data security requirements and the available security techniques calls for a new PLS approach that can prevent data recording to avoid off-line processing, provide stealth transmission, and enable scalability that complies with the highest data transmission rates. Furthermore, the new era of quantum computers implies that there may always be an intimidating computing power that may break any pure digital encryption code. Thus, the most troubling threat becomes "record now, decipher later."

Here, a novel all-optical PLS technique is presented in which the signal is optically decomposed into a noise-like signal, and the possibility of its recording is eliminated [5, 6]. In turn, digital post-processing and traffic analysis cannot be applied by the eavesdropper. Furthermore, enhanced immunity to man-in-the-middle attacks as well as jamming is provided. In addition, the proposed scheme enables stealth transmission (steganography), while the data can be concealed below the optical noise level in both time and frequency domains. The only way of retrieving the transmitted data at the receive side is by all-optically recomposing the signal by inversely applying all-optical actions opposite to the all-optical manipulations that were applied by the transmitter. Otherwise, the signal is destroyed during the optical detection and sampling process, with no possible improvement. Thus, such a system forces the eavesdropper to decode the encrypted data "on the fly" or to record a complex optical signal of multi-THz bandwidth under extreme (negative) OSNR conditions, which is effectively unrealistic.

2. PLS - Spread Spectrum and Multi-Homodyne Coherent Detection

The all-optical PLS system scheme is presented in Figure 1. The PLS method is based on the following photonic-tripod manipulation: (1) multi-THz optical spectrum spreading by the use of a mode-locked laser (MLL), (2) optical phase encoding by applying an encryption code forming the optical key, and (3) generating negative OSNR conditions by burying the optical signal below strong amplified spontaneous emission (ASE) noise source. In turn, this photonic-tripod manipulation results in a "noise-like" signal transmission spanned over multi-THz analog bandwidth. Detection and recording of the signal require a priory knowledge of the optical key, or a coherent receiver with multi-THz analog bandwidth, else, the signal will be destroyed and lost during the detection and sampling process.

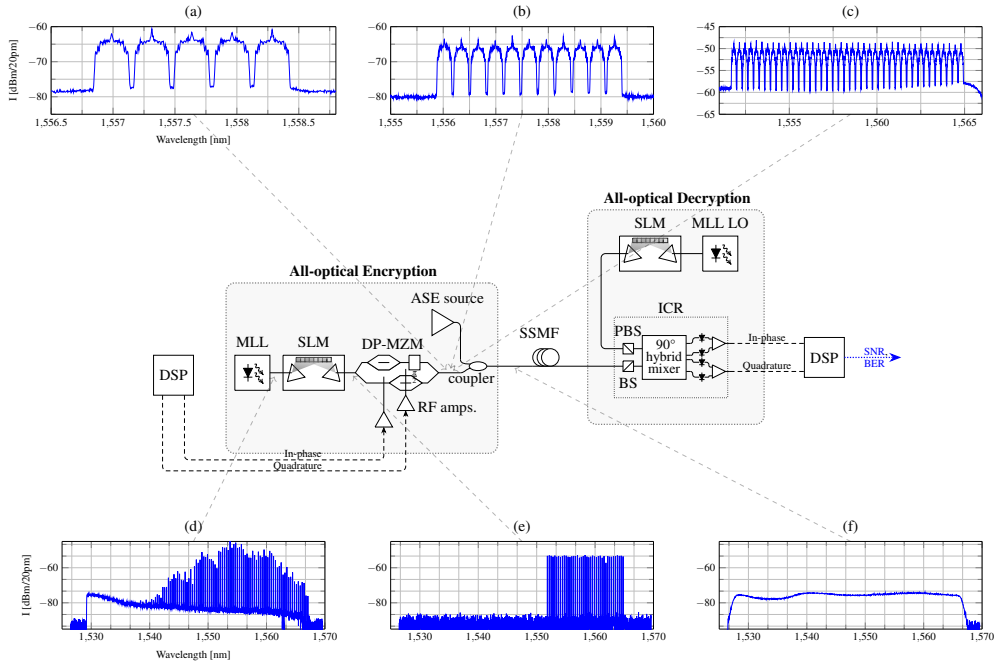
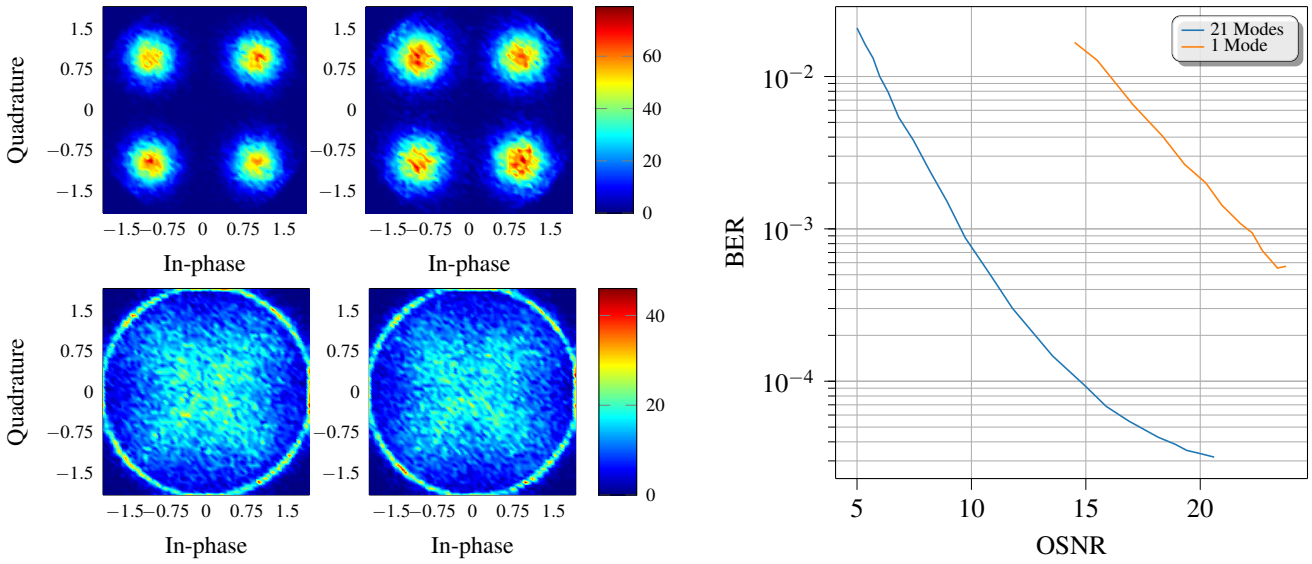


Fig. 1: Encrypted and stealthy coherent optical communication system. Conventional coherent modulator, coherent receiver, and coherent digital signal processor (DSP) are combined with optical encryption elements, forming an all-optical encryption system. Insets (a)–(c) represent the filtered, flattened, encoded, and modulated spectrum for 5, 11, and 41 comblines, respectively. Insets (d)–(f) represent the stealthy and encrypted transmitter flow: (d) MLL raw spectrum, (e) filtered and equalized 41 comblines generating 1.67 THz optical carrirers spectrum, and (f) modulated and buried under ASE noise (OSNR= -4dB) full C-band trace.

The eligible receiver must perform all-optical manipulations, opposite to the PLS transmitter manipulations. This is performed by multi-homodyne coherent detection (MHCD) process. An optical MLL like the transmitter MLL is used as a local oscillator (LO)-MLL. Optical mixing occurs between the transmitter-MLL and LO-MLL, resulting in multiple homodynes between the multiple mode pairs of the two lasers. By matching the phases between all the modes pairs, i.e., via optical key matching, coherent addition of the optical fields is performed at the photodetection process. In turn, optical-to-electrical processing gain is obtained, obeying square law detection. Thus, the eligible receiver gains processing gain proportional to the square of the number of mode pairs. For example, for N=100 modes MLL, the photodetection current will experience a processing gain of $N^2 = 10,000$. Simultaneously, the optical ASE noise experiences incoherent addition during photodetection, thus the ASE-related electrical noise will experience only N=100 times gain. Consequently, the optical-to-electrical conversion performs a processing gain of $N = 100$ thanks to the coherent addition process of the eligible receiver signal. The coherent addition occurs only conditional to the phase matching between each of the mode pairs of the transmitter and LO-MLLs, i.e., optical key matching. Thus, the receiver must have in hand the optical encryption key code in advance, in order to match the LO-MLL phases to the transmitter-MLL phases. Furthermore, if the encryption key code varies dynamically, the receiver must dynamically change the phase matching in real-time, on the fly. Conversely, the adverse user has a limited time to perform optical trials for code breaking of the optical key, up to the point when the code changes. No signal can be recorded and digitized if the optical key is not in hand.

3. Demonstration and Results

An inclusive transmission sub-system of the photonic-tripod PLS is depicted in Figure 1. saturable absorber (SA) semiconductor-based MLLs generate both the transmitter and receiver LO spread spectrum optical carriers. At the transmitter side, a spatial light modulator (SLM) encodes the optical key by phase modulating each comb-line independently, followed by the high-speed data modulation imposed by a coherent optical dual polarization quadrature amplitude modulation (QAM) modulator. At the transmitter output, the modulated and encoded MLLs signal is attenuated and “buried” under optical noise generated by an ASE noise source. At the receiver side, the LO-MLL is phase-encoded by an additional SLM according to the optical key of the received signal. The input optical encoded signal and the matched-encoded LO signal are mixed at an integrated optical coherent receiver, experiencing MHCD as explained in the Detection section above. In turn, following the coherent addition



(a) constellation diagram at the PLS sub- system receiver output
top - eligible
bottom - ineligible

(b) caption of last image
second line

Fig. 2: caption of main figure

processing gain, the signal is successfully retrieved at the receiver output.

Figures 1 and 2 summarize the measurements and results of the PLS sub-system demonstration. Fig. 1 c presents the transmitted spread spectrum after dual polarization quadrature phase shift keying (DP-QPSK) modulation at 33Gbaud. The repetition rate of the MLL is 40 GHz, and a total of 41 modes is being observed in this example. In Fig. 1f, the spectrum of the transmitted signal at the output of the PLS sub-system is depicted. No information is being observed, rather, a noise-like signal is seen. Fig. 2a presents the constellation diagram at the PLS sub-system receiver output for the cases of the eligible user (top) and the ineligible user (bottom). In the eligible user receiver, a clear DP-QPSK constellation is observed, while the ineligible user fails to detect any information. A quantitative sensitivity comparison of bit-error ratio (BER) versus OSNR between a single mode user versus 21 modes MHCD user is presented in Fig. 2b. It is observed that at the 5E-2 pre-FEC BER threshold, the required OSNR of the MHCD user is 13dB lower than that of the single mode user, indicating a successfully measured photonic processing gain of 13dB associated with the coherent addition engine exploited by the eligible user only.

4. Conclusion

Quantum computing era calls for new generation of post quantum security. Complementary to the new generation of quantum resilient cryptographic algorithms, a photonic layer security scheme is presented, which prevents the possibility of recording the encrypted signal prior to all-optical deciphering. Consequently, the threat of "record now and decipher later" is eliminated, adding a "photonic shield" towards post quantum secured systems.

References

1. K. Shaneman and S. Gray, "Optical network security: technical analysis of fiber tapping mechanisms and methods for detection & prevention," in *IEEE MILCOM 2004. Military Communications Conference, 2004.*, vol. 2 (2004), pp. 711–716 Vol. 2.
2. D. J. Bernstein and T. Lange, "Post-quantum cryptography," Nature **549**, 188–194 (2017).
3. A. Argyris *et al.*, "Chaos-based communications at high bit rates using commercial fibre-optic links," Nature **438**, 343–346 (2005).
4. X. Chen *et al.*, "Experimental demonstration of a 4,294,967,296-qam-based y-00 quantum stream cipher template carrying 160-gb/s 16-qam signals," Opt. Express **29**, 5658–5664 (2021).
5. E. Wohlgemuth *et al.*, "Stealth and secured optical coherent transmission using a gain switched frequency comb and multi-homodyne coherent detection," Opt. Express **29**, 40462–40480 (2021).
6. E. Wohlgemuth *et al.*, "A field trial of multi-homodyne coherent detection over multi-core fiber for encryption and steganography," J. Light. Technol. **41**, 2723–2735 (2023).