Secure optical communication using symbol-by-symbol time-domain spectral phase encoding with QPSK modulation

K. Wang[1], X. Tang[2], A. Wonfor[2], R. J. Collins[1], G. S. Buller[1], R. Penty[2], I. White[2], X. Wang[1*]
[1]*Institute of Photonics and Quantum Sciences, School of Engineering and Physical Sciences, Heriot-Watt University, Edinburgh, EH14 4AS, United Kingdom*
[2]*Centre for Photonic Systems, Electrical Engineering Division, Department of Engineering, University of Cambridge, 9 JJ Thomson Avenue, Cambridge CB3 0FA, United Kingdom*
Email address: x.wang@hw.ac.uk

Abstract: We report the experimental demonstration of a secure optical communication system using 40 Gbps coherent quadrature phase shift keying modulation. The security is implemented in physical layer using symbol-by-symbol time domain spectral phase encoding.

OCIS codes: 060.0060, 060.2330.

1. **Introduction**

As ever-increasing amounts of digital data are transmitted globally over the optical communication network, ensuring the security of the optical communication system becomes an increasing priority. In current communication systems the security measures are mainly implemented in higher layers by encryption methods (such as AES). The strength of the security is determined by the computational difficulty of breaking the encryption algorithms. Bit-by-bit time-domain spectral phase encoding (TDSPE) technique is one effective technique to implement security in the physical layer of modern conventional optical communication systems. It scrambled the optical signal in both spectral and time domains into noise-like signals using random patterns [1-4]. In a bit-by-bit TDSPE secured optical communication system, the security section was separated from data modulation. The scrambling code was used to encode the stretched and overlapped signal pulse for transmission. The code rate was normally larger than the pulse repetition rate.

Previously, TDSPE has been demonstrated using on-off keying (OOK) and differential phase shift keying (DPSK) modulation using direct or differential detection at up to 40 Gbps data rate [2]. Using higher order modulation schemes such as quadrature phase shift keying (QPSK) or quadrature amplitude modulation (QAM) and coherent detection, it is possible to achieve even higher speed secure optical communication using TDSPE. In this paper we implement a high speed secure optical communication scheme using TDSPE to physical layer security in one communication system. We experimentally demonstrate a 40-Gbps coherent QPSK transmission with symbol-by-symbol code scrambling.

2. Principles of operation and experimental setup

2.1 Theoretical model

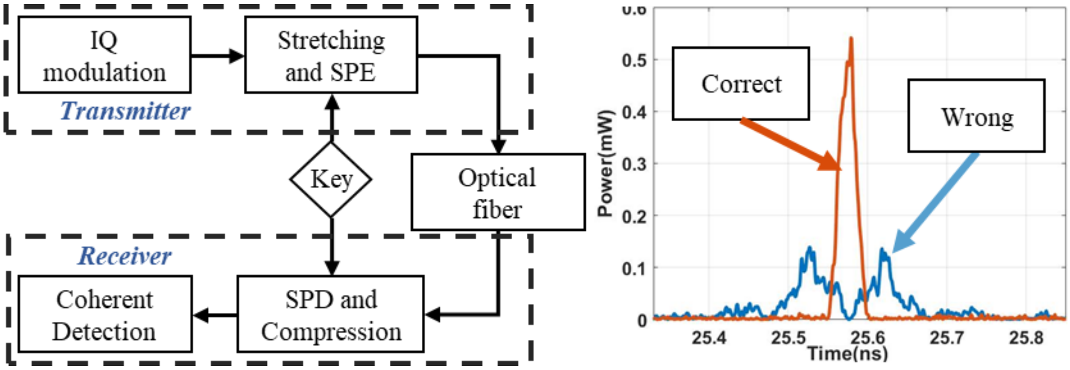

Fig. 1. (a) Operating principles of the secure communication scheme and (b) the correctly/wrongly decoded optical pulse (after dispersion compression).

The operating principles of the scheme are depicted in Fig.1(a). At the transmitter, the optical pulse, carrying the QPSK data, is temporally stretched by a highly dispersive element, and the TDSPE is executed using a high-speed phase modulator driven by scrambling code patterns [1], which is assumed to be securely shared between transmitter and receiver. Assuming that the width of the stretched pulse is $\mathbf{T_s}$, and the duration of each scrambling code chip is $\mathbf{T_c}$ (the code rate is $1/\mathbf{T_c}$). Thus, the length of the scrambling code applied on each stretched pulse is $\mathbf{T_s}/\mathbf{T_c}$. The transmitted signal in the classical channel (i.e. optical fiber) appears noise-like. If the signal is wrongly decoded by an unauthorized user, the signal will remain noise-like over an extended period (as shown in Fig.1(b)) and so the encoded information cannot be extracted. For a sufficiently long code, the probability of successfully randomly guessing the code at the time of measurement is infinitesimally small. The extension in time of the wrongly decoded optical pulse is proportional to $\mathbf{T_s}/\mathbf{T_c}$ [2]. Therefore, increasing this ratio enhances the security performance of the system. $\mathbf{T_s}$ is determined by the total stretching dispersion and optical carrier's bandwidth and $\mathbf{T_c}$ is relevant to the encoding speed.

2.2 Experimental setup

The experimental setup is shown in Fig.2. A 20-GHz optical pulse train was generated by intensity modulating the signal from a 1551.2-nm continuous-wave (CW) laser source with an extinction ratio of ~20.7 dB. The QPSK data was modulated to the shaped pulse train by an in-phase quadrature (I-Q) modulator at a symbol rate of 20 Gbaud. After the data modulation, the 10-dB bandwidth of the pulse was around 0.167 nm. The total dispersion of the dispersion compensated fiber (DCF) was -1498 ps/nm, and thus the optical pulse was stretched to ~200 ps time duration. The 16.67-GHz spectral phase encoding (SPE) introduced 4 chips into each stretched pulse by a phase modulator (PM). The encoded signal was launched into a classical channel comprised of 52.3 km of standard telecommunications single mode optical fiber (SMF) for transmission. After transmission, a subsequent span of DCF was used to compensate for the dispersion caused by the SMF. The relative delay of the electrical and optical signal was adjustable to synchronize the optical signal and the decoding pattern.

The compression dispersive element was not needed in the experiment as the coherent receiver was able to detect both quadrature and in-phase parts of the signal to compensate the dispersion using digital signal processing (DSP) [5]. This approach improves the received signal power relative to the alternative of using SMF to physically compensate the remaining dispersion.

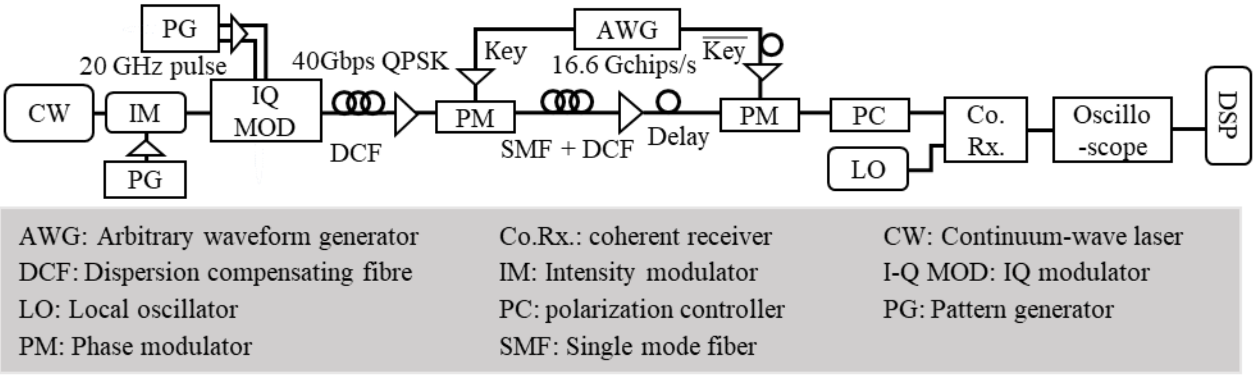

Fig. 2 The schematic plot for the classical communication channel in the experiment

3. Results and discussion

3.1 Back-to-back (B2B) system with TDSPE scrambling

With the transmitter and receiver directly connected, the error vector magnitude (EVM) and bit error rate (BER) were firstly tested to evaluate the transmission property and security performance. The signal constellation diagram is shown in the Fig.3 (a)&(b). The data length used in the experiment was 2^{15}-1, therefore the lowest measured BER was ~3×10^{-5}.

In Fig.3(a) and (b), if the received signal was decoded correctly, the EVM was 18%, and there was no error detected. However, for the incorrect decoding case, the EVM and BER were 101% and 0.28 respectively, which indicated that the data were hidden in the noise-like signal and could not been recovered. The recovered symbols with the phase state of '$\pi/4$' are marked for both correct decoding and incorrect decoding cases in the figure to show the comparison. One can clearly see that the incorrect decoding was used, the signal's symbols were spread over the diagram and therefore could not be recovered. Fig.3(c) compares the spectra of the correctly and incorrectly decoded signals. The spectrum of the correctly decoded signal resembled that of the original data as the scrambled spectral phases were correctly recovered in the decoding. The mismatch between the two is attributed to the imbalance of the PMs' depth used in the encoding and decoding operations and the synchronization timing error caused by the non-ideal delay lines used in the experiment. The incorrectly decoded signal exhibited a much broader spectrum compared to the original and the correctly decoded signals, showing that the signal remained noise-like and thus it was not possible to recover the original data.

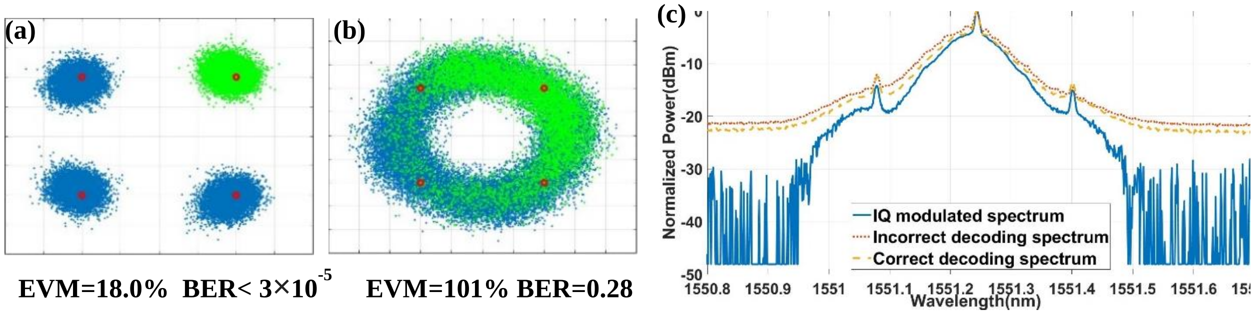

Fig. 3 The signal constellations for the seeded B2B system in the cases of correct decoding (a) and incorrect decoding (b), and the spectral comparison (c) for both cases.

3.2 Transmission experiment

Fig.4 shows the EVM and BER results after transmitting through the 52.3 km SMF. Because the signal had suffered from critical loss in the transmission fiber, the EVM had increased to 30% for the correctly decoded signal, but the transmission error was still below 3×10^{-5}. Fig.4(b) clearly shows that both the phase and amplitude of incorrectly decoded signal could not be recovered, because of the low signal-to-noise ratio resulted by the transmission.

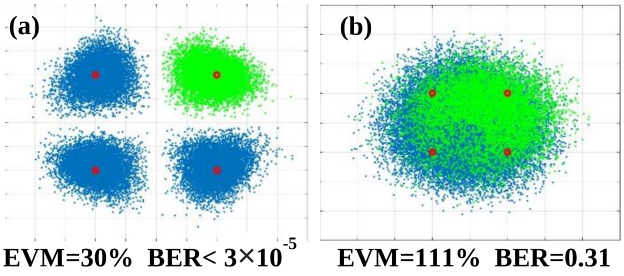

Fig. 4 Signal constellations for the transmission experiment for (a) correctly decoded and (b) wrongly decoded signal

4. Conclusion

We have demonstrated a secure 40-Gbps communication scheme over 53 km using TDSPE with the code scrambling encryption and decryption. We experimentally investigated the transmission and security performance of the system, and verified that the transmitted QPSK data could only be successfully recovered for an authorized user with the correct code. The proposed scheme could be further integrated with quantum key distribution to provide the code being securely shared between transmitter and receiver.

5. Acknowledgements

The authors acknowledge the support of the EPSRC Quantum Technology Hub in Quantum Communications (reference EP/M013472/1).

6. References

[1] X. Wang, Z. Gao, Xuhua Wang, N. Kataoka, et al, "Bit-by-bit optical code scrambling technique for secure optical communication", Optics express, **19** 3503–3512(2011).

[2] Z. Gao, B. Dai, X. Wang, et al, "40 Gb/s, secure optical communication based upon fast reconfigurable time domain spectral phase en/decoding with 40 Gchip/s optical code and symbol overlapping", Optics letters, **36**, 4326–4328(2011).

[3] X. Wang, Z. Gao, N. Kataoka, et al, "Time domain spectral phase encoding/DPSK data modulation using single phase modulator for OCDMA application", Optics Express, **18**, 9879-90(2010).

[4] Z. Gao, B. Dai, X. Wang, et al, "10-Gbit/s, reconfigurable time domain SPE-OCDMA system with code shifting and pulse overlapping", Microwave and Optical Technology Letters, **54**, 808-810(2012).

[5] T. Xu, G. Jacobsen, S. Popov, et al. "Chromatic dispersion compensation in coherent transmission system using digital filters", Optics Express, **18**, 16243-16257(2010).