40Gbits^{-1} Data Transmission in an Installed Optical Link Encrypted Using Physical Layer Security Seeded by Quantum Key Distribution

Kexin Wang, Xinke Tang, Adrian Wonfor, *Member, IEEE*, Robert John Collins, *Member, IEEE*, Gerald S. Buller, Richard V. Penty, *Senior Member, IEEE*, Ian H. White, *Fellow, IEEE*, and Xu Wang, *Senior Member, IEEE*

***Abstract*—Data security plays an increasingly important role in modern telecommunications. The advent of quantum computational processors presents a significant threat to today's widely employed public key encryption algorithms, necessitating the adoption of new approaches to data encryption. Whilst quantum key distribution guarantees unconditional security for cryptographic key exchange in optical communication networks, the data rate is slow (Mbit/s), especially when compared to conventional optical communication. Here we present a highly secure encryption approach in which the encryption key, generated by quantum key distribution at a rate of up to 2.9 Mbit/s, was used to seed physical layer encryption performed using time domain spectral phase encoding (TDSPE). This allowed us to demonstrate encrypted 40 Gbit/s quadrature phase shift keyed data communications over 52.3 km of installed optical fiber, which cannot be eavesdropped using brute force computational attacks. Any attempt to eavesdrop the encrypted signal in the physical layer is highly time-sensitive – the phase states must be measured and decrypted prior to optical signal attenuation, which means that the attack procedure typically needs to be completed within a few milliseconds. This work represents the first example of quantum-enhanced physical layer encryption at realistic optical data rates that is fully secure from brute force computational attacks and the first demonstration of TDSPE using continuous-wave laser source and quadrature phase shift key modulation.**

***Index Terms*—Optical fiber communication, communication system security, quantum cryptography.**

Manuscript received January 6, 2021; revised May 22, 2021 and June 21, 2021; accepted June 22, 2021. Date of publication July 8, 2021; date of current version October 4, 2021. This work was supported by the EPSRC Quantum Technology Hub in Quantum Communication Hub under Grants EP/M013472/1 and EP/T001011/1. *(Corresponding author: Xu Wang.)*

Kexin Wang, Robert John Collins, Gerald S. Buller, and Xu Wang are with the Institute of Photonics and Quantum Sciences, School of Engineering and Physical Sciences, Heriot-Watt University, Edinburgh EH14 4AS, U.K. (e-mail: kw34@hw.ac.uk; r.j.collins@hw.ac.uk; g.s.buller@hw.ac.uk; x.wang@hw.ac.uk).

Xinke Tang was with the Electrical Engineering Division, Department of Engineering, University of Cambridge, 9 JJ Thomson Avenue Cambridge CB3 0FA, U.K. He is now with the Robotics Research Center, Peng Cheng Laboratory (PCL), Shenzhen 518055, China (e-mail: tangxk@pcl.ac.cn).

Adrian Wonfor, Richard V. Penty, and Ian H. White are with the Electrical Engineering Division, Department of Engineering, University of Cambridge, 9 JJ Thomson Avenue Cambridge CB3 0FA, U.K. (e-mail: aw300@cam.ac.uk; rvp11@cam.ac.uk; ihw3@cam.ac.uk).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/JLT.2021.3095539.

Digital Object Identifier 10.1109/JLT.2021.3095539

I. Introduction

ENSURING the security of information exchange in optical communication systems has become one of the primary challenges in telecommunication networks. In current communication systems the security measures are mainly implemented in higher Open Systems Interconnection (OSI) network model layers by digital data encryption methods (such as Advanced Encryption Standard (AES) or Lightweight Encryption Algorithm (LEA) in the syntax layer). When data are encrypted using these upper-layer encryption methods, the transmitted encrypted data are composed of relatively high-intensity optical digital signals that could be easily measured and perfectly copied by an eavesdropper. After measurement, the eavesdropper can then attempt to break the encryption on the perfect copies, taking as long, or using as many copies, as is necessary. Therefore, the strength of the security is determined by the computational difficulty of breaking the encryption algorithms [1], which is often referred to as **computational security**. Quantum key distribution (QKD) is a proven method of generating and sharing verifiably secure keys between two users by using the properties of quantum mechanics [2]–[8]. The distributed secure keys can be then used in classical (i.e., non-quantum) data encryption protocols (such as the absolutely secure, but low key efficiency, one-time-pad) [2], [7]. However, the key generation rates are very low compared to the data transmission rates of classical communication systems and therefore real-time use of the key with low key efficiency encryption protocols is impractical. Consequently, there is a need to consider a compromise between the verifiable security of QKD or the enhanced data transmission rate with relatively reduced security offered by classical encryption processes.

The time-domain spectral phase encoding (TDSPE) technique was proposed as an effective and flexible method of implementing network security in the optical physical layer by rapid (bit-by-bit) encoding of the high-speed optical signal into a noise-like encoded signal [9]–[13]. Using TDSPE, the security is implemented optically in the physical layer, which could be referred to as **physical level security**. Security investigations of the spectral phase encoding (SPE) in OOK/DPSK (On-Off Keying/Differential Phase Shift) systems have indicated that the SPE could achieve mathematically variable security [14]. Consequently, no digital optical circuits (such as memory) exist

which can fully detect and maintain the optical signal with sufficient fidelity to permit an eavesdropping attack over a long-duration, say, of greater than 1 ms. In order to decrypt such encrypted data, an eavesdropper would either require full knowledge of the symmetric encryption key in advance or be able intercept the data and then attempt to randomly check the scrambling code **in real time**. In practice, the latter approach is very unlikely to be successful without the eavesdropper having *a priori* knowledge of significant parts of the key. The TDSPE scheme operates in the physical layer of the optical communication network, distinct from traditional symmetric-key encryption such as AES, which operates at the syntax layer [15], and is entirely transparent to upper-layer protocol/contents. The TDSPE scheme can, therefore, be layered with symmetric-key encryption to offer enhanced security.

In the bit-by-bit code scrambling TDSPE, the confidentiality of the encryption key or scrambling code (SC) is the essential aspect of the overall security of the communication system. Therefore, we propose a new approach that employs QKD to generate and share the secure keys which seed the coding operations used in the TDSPE to scramble the signal in the physical layer. In the work reported here, the cooperative integration of QKD and TDSPE implements system physical level security in an optical communication system. The QKD system provides verifiable security to the generation of secure keys between two authorized parties. The quantum key then serves as a seed to generate the SC for TDSPE. The code scrambling is able to operate bit-by-bit at a high clock rate (demonstrated from 20 GHz to 40 GHz [9]–[13]) in the TDSPE system acts as an interface between QKD and the classical optical transmission system, and enables a further improvement to the security of high-speed optical communication, compared with digital data encrypted systems. The TDSPE stage could be regarded as a modular "Plug and play" security system used to improve the security of the traditional optical communication systems. The full protocol will be discussed Section II.

Previously, TDSPE had been demonstrated using a single phase modulator to perform both TDSPE encoding and differential phase shift keying (DPSK) data modulation [10]. Bit-by-bit code scrambling has been further demonstrated at up to 40 Gbps data rate for OOK and DPSK data formats with improved security and flexibility of the SPE codes [10]–[13]. High order coherent modulation techniques such as quadrature phase shift keying (QPSK) and quadrature amplitude modulation (QAM) have been widely adopted in optical communication systems [16], and various types of algorithms could be applied in the digital signal processing (DSP) stage [17]. However, the compatibility of TDSPE with these coherent high order modulation techniques has not been considered in the previous investigations.

Spectral encoding requires a broad spectral bandwidth to facilitate the encoding. Although an intensity modulated continuous-wave (CW) laser is commonly used in practical optical networks, previous TDSPE schemes employed a high-speed bandwidth-limited optical pulse as the signal carrier due to its broad spectral bandwidth [10]. However, the TDSPE scheme with a high-speed short pulse source is not compatible with most practical optical fiber transmission systems that use CW optical sources, and this type of laser source is very expensive. It is highly desirable to use a CW source for the TDSPE scheme to get higher compatibility.

This paper proposes and demonstrates a novel integrated QKD seeded TDSPE scheme. TDSPE operating with QPSK modulation using CW laser source is also firstly demonstrated to provide physical layer security with full compatibility with the traditional symmetric-key encryption. A proof-of-principle experiment was demonstrated physical layer security in a 40G-Gbps coherent QPSK transmission system using a CW laser. The quantum key distribution element of this integrated system was demonstrated using a deployed link in the Cambridge Quantum Network [18]. The TDSPE system used the seed keys generated by the QKD system. Investigations on transmission and security performance were also carried out. The classical 40 Gbps QPSK data transmission system, using single wavelength and single polarization, transmitted data over 52.3 km of standard telecoms single-mode fiber (SMF).

II. Operating Principles

A. Protocol

The operating principles of the proof-of-principle experiment is shown in Fig. 1. Following the optical transmitter, the physical layer encoding was applied to perform TDSPE. This was driven by the SC patterns which were generated by the distributed quantum keys as shown in Fig. 2. This protocol provides enhanced security performance in the physical layer via a QKD seeded TDSPE scheme and is fully compatible with security protocols operating in other OSI layers. It is important to emphasize that any security scheme in the syntax layer, e.g. AES, is available to be introduced into this protocol for further security performance.

The quantum key distribution and data transmission procedure is shown in Fig. 2. At the beginning of the transmission process, the quantum key was first generated, distributed, and stored by the two authorized parties, Alice and Bob (Fig. 1). The SC pattern was derived by pseudo random number generation algorithms seeded by the quantum key, which could only be successfully recovered by the complementary code pattern generated from the same key by the same pseudo random number generation algorithm. The signal frame was divided into synchronization header, guard header gap, data frame, and guard tail gap. The synchronization header was used to synchronize the beginning of the signal frame and the physical layer encoding. The guard header and tail gaps in the data frame were filled with random symbols to provide sufficient scrambling for the first and last symbols.

The generated SC pattern with length $\mathbf{L_d}$ (shown in Fig. 2) was used to fully mask the data frame at the code rate of $\mathbf{R_c}$ via TDSPE. The duration of the QKD phase ($\mathbf{T_{Key}}$) and data transmission phase ($\mathbf{T_{Data}}$) are given by

$$\mathbf{T_{Key}} = \mathbf{N_k} \,/\mathbf{R_k} \tag{1}$$

$$\mathbf{T_{Data}} = \mathbf{L_d} \,/\mathbf{R_c} \tag{2}$$

where $\mathbf{N_k}$ and $\mathbf{R_k}$ are the block size of quantum keys and bit rate of the QKD system, respectively. In Fig. 2, $\mathbf{T_Q}$ and $\mathbf{T_D}$ are the

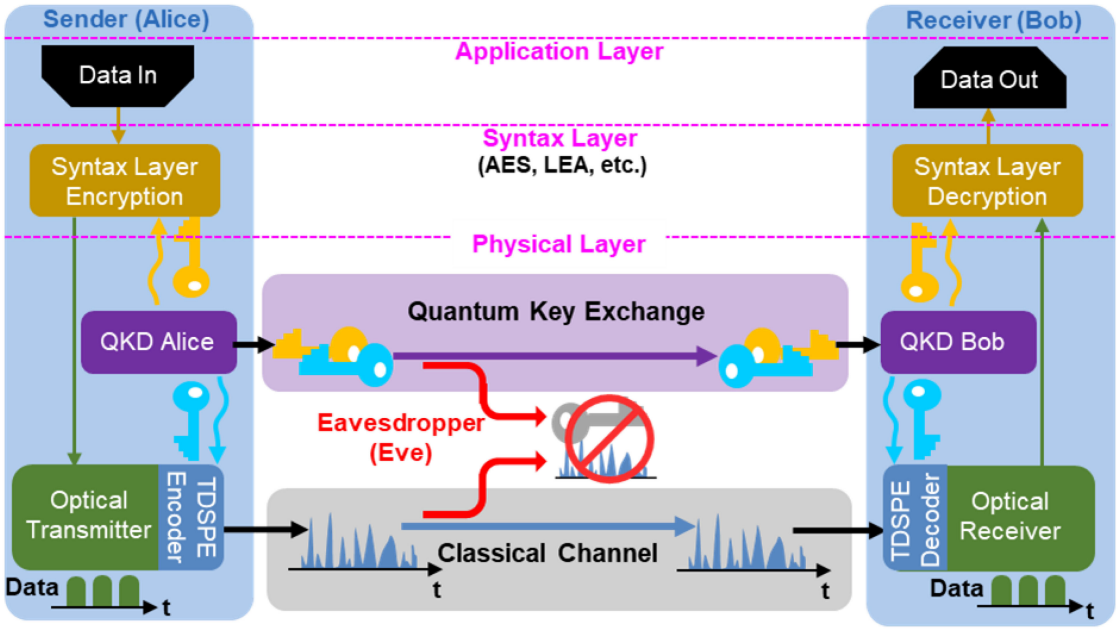

Fig. 1. Operational principles of the QKD seeded physical layer encoding security scheme.

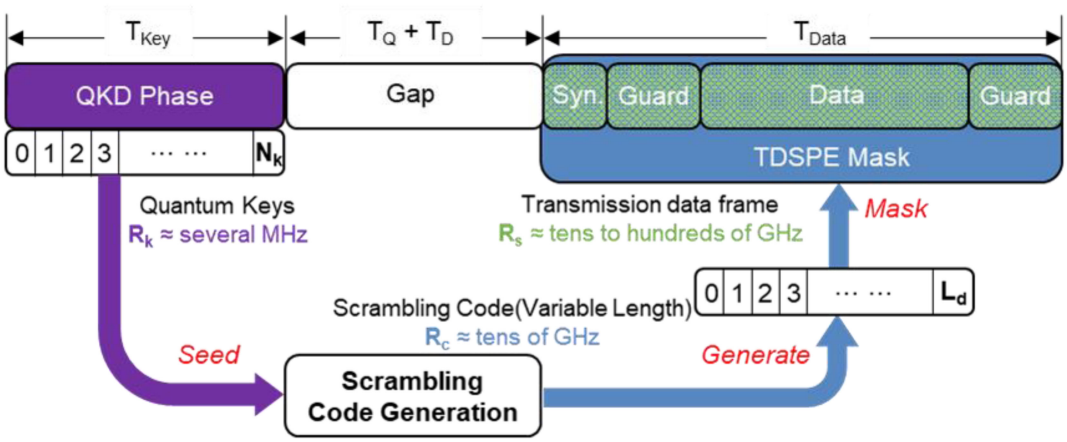

Fig. 2. The procedure of the SC generation from the distributed quantum key under the operation protocol of the QKD seeded TDSPE security scheme, which also depicts the frame structure of the classical signal. 'Syn.' is the synchronization header for a data frame. The setup and post processing ($\mathbf{T_Q}$ and $\mathbf{T_D}$) are located at the beginning and end of each phases.

time for setup and post processing for the quantum and classical systems respectively. The calculated ratio between quantum bits and classical bits is given by

$$\mathbf{R_{KB}} = \mathbf{N}_k / \left(\mathbf{L_d R_s / R_c} - \mathbf{N_s} - 2\mathbf{N_g}\right) / \log_2(\mathbf{M}) \quad (3)$$

where $\mathbf{M}$ is the number of levels for a M-ary modulation, i.e. $\mathbf{M} = 2$ for DPSK and $\mathbf{M} = 4$ for QPSK, and the code is then used for the physical layer encoding. $\mathbf{N_s}$, $\mathbf{N_g}$, are the number of symbols in the synchronization header and guard gaps, respectively. $\mathbf{R_s}$ is the symbol rate in the data transmission. The scrambling code rate ($\mathbf{R_c}$) is adjustable by using different encoding rate for the TDSPE, so it could reach tens of gigahertz. The $\mathbf{R_{KB}}$ in the experiment (shown in Fig. 4) was around 0.42. However, as will be presented in the following sections, the quantum key (or scrambling code) is working on the dispersively stretched optical pulses instead of classical bits in the TDSPE scheme. And the ratio between quantum keys and optical pulses was approximately 0.83.

An eavesdropper, Eve, who knows the code generation algorithms but does not have knowledge of the key for physical layer encoding, could only access a noise-like signal which is scrambled by the TDSPE. An analysis of the security of the system will be presented in Section V.

B. *Symbol-by-Symbol TDSPE With CW Optical Source*

As the QKD process offers verifiable security for the seed key, the security of the data transmission in the classical channel

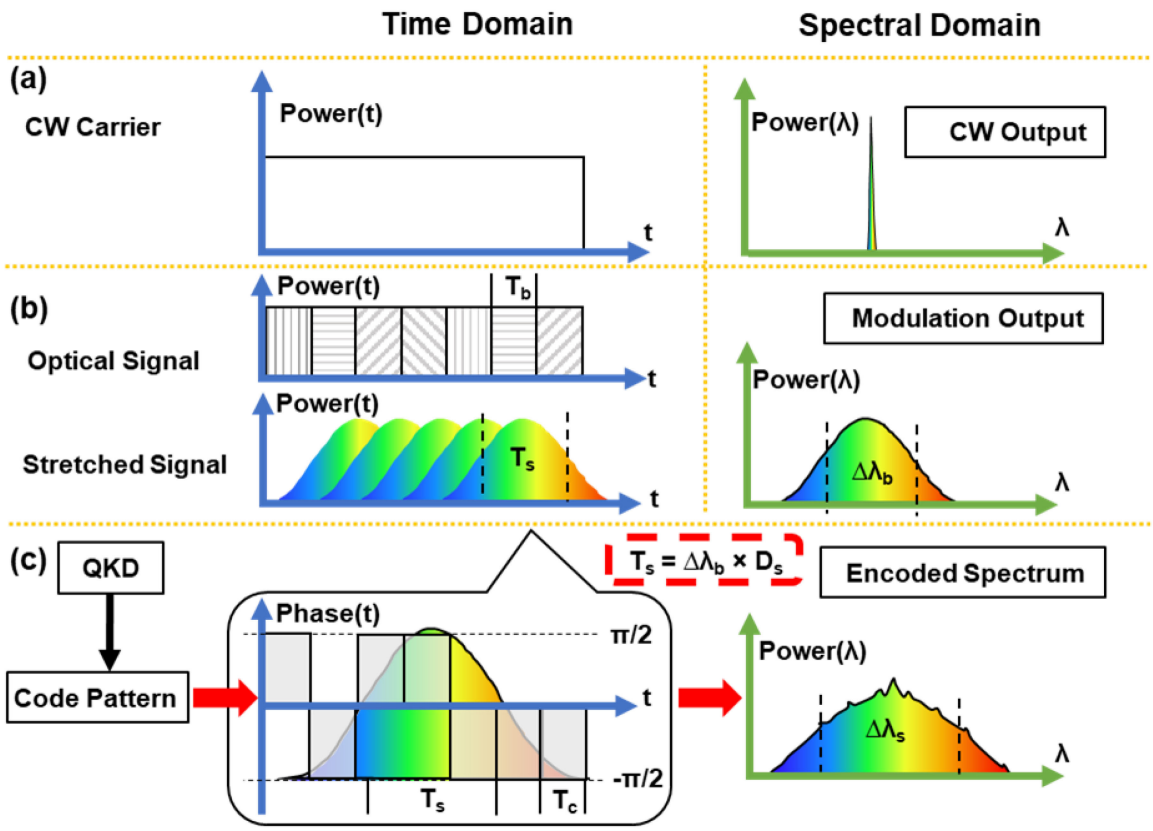

Fig. 3. The operating principles of TDSPE scrambling in both time domain and spectral domain. (a) Waveform of the continuous-wave carrier and its spectrum (with the linewidth of several hundred kilohertz). (b) The stretched optical signal in each bit being modulated by the transmission data and its spectrum (the spectral bandwidth is significantly broadened to $\Delta\lambda_b$). (c) Phase encoded optical signal by the scrambling code pattern generated from the QKD and its spectrum (bandwidth is further broadened to $\Delta\lambda_s$).

is determined by the security of the TDSPE. Since receiver Bob possessed the key, he was able to access the correctly decoded optical signal (CDOS) while eavesdropper Eve lacked the knowledge of the SC to perform the correct decoding and detected a wrongly decoded optical signal (WDOS).

Fig. 3 illustrates the operating principles of the proposed TDSPE scheme using a CW laser source. The QPSK data was loaded on to the CW optical carrier by in-phase/quadrature (IQ) modulation. The optical spectrum of the QPSK signal was broadened to $\Delta\lambda_b$ after TDSPE. For each symbol, the dispersive element stretched the signal in the time domain and different wavelength components were located at different time slots. Therefore, each symbol was stretched and overlapped with adjacent bits as shown in Fig. 3(b).

The stretched signal had duration ($\mathbf{T_s}$) which can be calculated from knowledge of the dispersion ($\mathbf{D_s}$) and the signal's bandwidth ($\Delta\lambda_b$) thus:

$$\mathbf{T_s} = \mathbf{D_s} \cdot \Delta\lambda_b \tag{4}$$

The SPE was executed by the phase modulator driven by the SC pattern with frequency of $\mathbf{R_c} = 1/\mathbf{T_c}$. Through the TDSPE process, the SC pattern became a sequence of phase shifting for the stretched optical symbols. The number of codes encoded onto a stretched optical symbol ($\mathbf{N_c}$) can be calculated by:

$$\mathbf{N_c} = \mathbf{T_s}/\mathbf{T_c} \tag{5}$$

A larger $\mathbf{N_c}$ results in the longer duration of the WDOS symbol, which means lower optical signal-to-noise ratio (OSNR), which is beneficial for protecting the signal from unauthorized detection [13].

Each optical symbol experienced different SC patterns, resulting in symbol-by-symbol code scrambling, and the bandwidth of the scrambled signal spectrum ($\Delta\lambda_s$) was also broadened, compared with the bandwidth of the original QPSK signal ($\Delta\lambda_b$). We will further discuss this effect in the symbol-by-symbol TDSPE by simulation and experimental results in section IV.

In a TDSPE masked data frame, a target symbol was affected by the overlapping scrambling from adjacent symbols while it is being encoded by the SC. However, adjacent symbols undergo the same experience with the target symbol, so the whole data frame experiences this 'domino-effect' scrambling, and, for a successful eavesdropping, it is required to correctly decode the whole data frame to remove the overlapping scrambling, as will be discussed in Section V. The QPSK symbols, which were only affected by the code scrambling, were separately simulated and discussed in Section IV.

In the proposed system, the header and tail guard gaps are essential to enhance the security for the first and last symbols

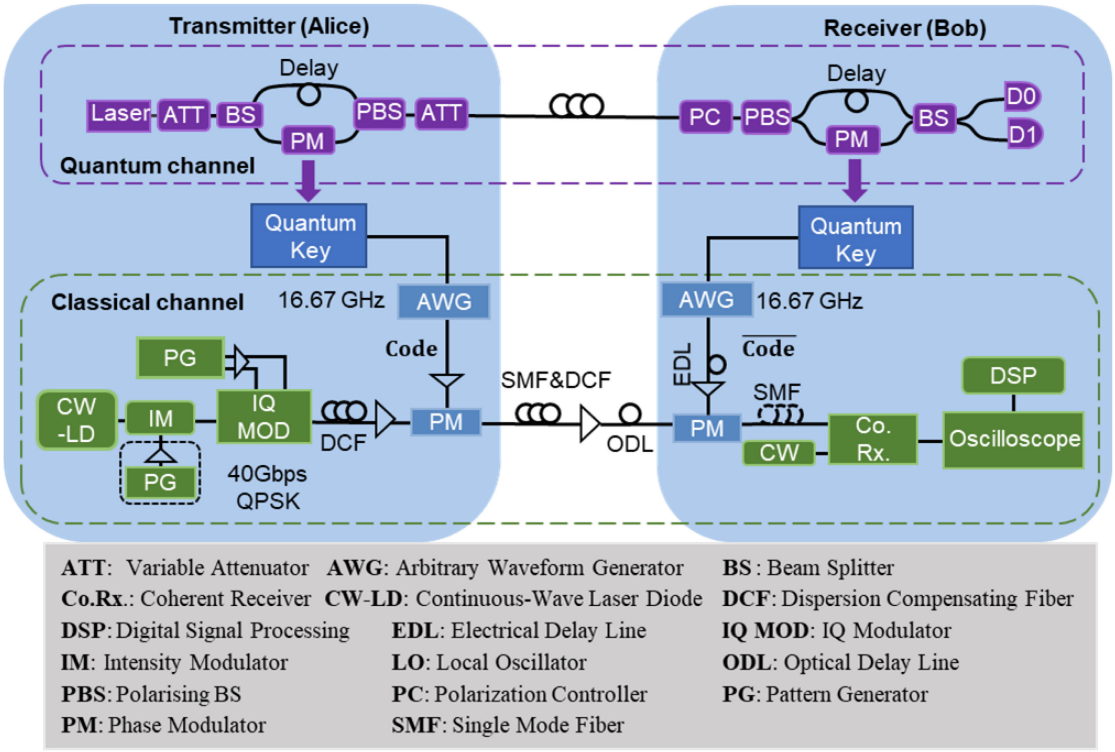

Fig. 4. Schematic plot for the classical communication channel and QKD channel. An overbar denotes logical (binary) inverse.

in the data frame, which have the least code scrambling and overlapping scrambling. In the case of correct decoding, the gaps can be easily removed. Otherwise, symbols in the gap would spread out over and impact the recovery for the first and last symbols. To maximize the security performance, the number of gap symbols ($\mathbf{N_g}$) should be equal to or larger than the ratio $\mathbf{T_s/R_s}$.

III. System Setup

A. Classical Channel

A schematic of the experiment and simulation system is shown in Fig. 4. An optical carrier was generated by a 1551.2 nm wavelength CW laser diode (CW-LD) of linewidth less than 100 kHz. The CW light was pulsed by an intensity modulator (IM) driven by the pattern generator (PG) and its driver (surrounded by the thin dark dashed line in the left-hand block), which was only enabled for the pulsed-laser cases. The electrical output generated by the PG was a pulse train with a FWHM of 25 ps and repetition rate of 20 GHz. The QPSK data was modulated onto the carrier by an IQ modulator (IQ MOD) at the symbol rate of 20 Gbaud. The modulated signal was stretched by a dispersion compensated fiber ($\mathbf{D_s} = -1498$ ps/nm) to 374 ps. The stretched QPSK symbols was encoded by the 16.67 GHz TDSPE, which used Alice's key to derive the SC. The SC pattern was generated by the arbitrary waveform generator (AWG). In this configuration, $\mathbf{N_c}$ in (5) was approximately 6. After the TDSPE, the signal was launched into a 52.3 km standard telecommunications single mode optical fiber (SMF) which served as the classical channel in the experiment, where the total launch power of the classical transmitter is around 0 dBm. A subsequent span of DCF at the receiver's side was used to compensate for the dispersion introduced by the SMF. The electrical and optical delay lines (EDL and ODL respectively) were used to manually synchronize the relative delay of the decoding (electrical) and received (optical) signal. The synchronized optical signal was decoded by the complementary SC pattern, which was derived from Bob's key. After decoding some dispersion remained in the signal, introduced by the DCF in the encoding system, and this could be compensated by the DSP in coherent detection [19]. Therefore, dispersion compensation before the coherent receiver was not necessary in the experiment. By this approach, the detected signal power could be improved relative to the alternative of using SMF to physically compensate the remaining dispersion. Finally, the optical signal was coherently detected by a coherent receiver (Co. Rx.). The distributed secure key and SC were in one-to-one correspondence. Due to the experimental conditions, the proposed scheme was demonstrated by a laboratory transmission experiment with the loopback quantum keys, which were generated by the QKD system operating over an installed fiber loopback terminating at the CAPE Node of the Cambridge Quantum Network. The distributed keys were than used for the Alice's encoding and Bob's decoding.

In the experimental configuration, the length of synchronization header was 2048 symbols duration. The two guard gaps in the data frame were filled by a set of random QPSK symbols and their length was 8 symbols duration. Each data frame contained 32768 QPSK symbols.

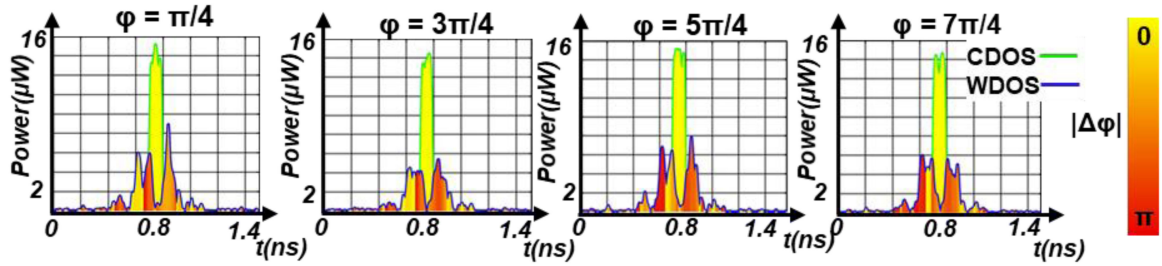

Fig. 5. The simulated amplitude and phase distribution carried by correctly decoded optical signal (CDOS) and wrongly decoded optical signal (WDOS) with different transmitted QPSK symbols.

B. The QKD System

Generation of the secure key was conducted using a Toshiba phase-encoded QKD system, which has been reported in [7], [20]–[22]. In Fig. 4(a), binary data is encoded onto weak-coherent states by Alice using phase shifts of $0/\pi$ or $+0.5\pi$/-0.5π. These are subsequently transmitted to receiver Bob. Bob applied a modulation of 0 or $+0.5\pi$ to the received signal and detected the result using single photon detectors D_0 and D_1. Asymmetric Mach-Zehnder interferometers were employed to perform the phase encoding/decoding. The quantum signal is detected by the single photon avalanche photodiodes operating in self-differencing mode used in the QKD receiver. The perturbation of the signal caused by an eavesdropper would result in an increase in the quantum bit error rate (QBER), which could be quantified by Alice and Bob. The system was operating under the BB84 protocol with two decoy states to achieve the maximized secure key rate. The intensity of the signal states was 0.4 photons per pulse while the intensities for strong decoy states and weak decoy states were 0.1 and $\sim 10^{-4}$ photons per pulse, respectively. A multithreaded version of the Cascade protocol [23] was used to perform the error correction. As there is a trade-off between efficiency and speed of the privacy amplification algorithm, the size of the large sifted block was 100 Mbit to minimize the finite key size effects. The implementation of privacy amplification used a number theoretic transform method. The security parameter for privacy amplification was 10^{-10} which suggests that the key failure probability was 1 key failure every 30,000 years when the secure key rate is 1 Mbps with a block size of 100 Mbits [18]. The synchronisation and reconciliation channels were wavelength multiplexed onto the same fiber as the quantum channel. The total launch power of these classical channels was around -12 dBm.

In the experimental setup the quantum channel was operated over a loopback in the installed fiber Cambridge Quantum Network. The employed quantum link length was around 21.2 km with an attenuation of about 7.8 dB. The secure bit rates were above 2 Mbps and the QBER was less than 2.5% during the transmission. Key distribution was carried out prior to the data transmission experiment and the key buffered since the key generation rate was low in comparison to the SC rate required for TDSPE. The key refresh rate for the TDSPE was determined by the length of secure key and generated SC, and this can be changed by applying different SC generation algorithms.

C. Simulation

The symbols' amplitude and phase distribution results (Fig. 5) was simulated using a combination software from VPIphotonics and custom analysis routines written using MatLab. The system model was built in the VPIphotonics and the signal processing was performed in the Matlab. The modelled system followed the same configuration as the experimental system (Fig. 4), including the device loss and the response bandwidth. The sampling rate and data rate of the simulation model were 1.28 TSa/s and 1024 bits respectively, where the sampling rate was necessary to be sufficiently high to calculate the amplitude and phase information of the signal carrier. To ensure that the detail of the scrambling effect was rendered accurately, the simulation model was done by using the single QPSK symbol.

D. Digital Signal Processing

The digital signal processing employed in this work was the standard algorithm for the optical coherent QPSK signal [17], which consists of the signal calibration, dispersion compensation, constant modulus algorithm, frame synchronization, and carrier phase estimation.

IV. Simulation And Experimental Investigation

A. Simulation Result

The scrambling effect on different QPSK symbols were simulated and are presented in Fig. 5. In the optical coherent QPSK system, the data recovery performance is determined by the quality of detected amplitude and phase of the optical signal. Fig. 5 shows both the amplitude and phase of different decoded QPSK symbols. The CDOS and WDOS are plotted using green and blue outlines, respectively. The colours of the shading under the lines show the phase differences ($|\Delta\varphi|$) of the signal with respect to the transmitted phase state (φ) using the colour scale below Fig. 5. The simulation results clearly show that the CDOS has a well-defined waveform with correct phase information carried by the optical signal (no phase error), while the WDOS exhibits a noise-like low intensity waveform with random phase distribution over an extended period for both amplitude and phase (phase error randomly distributed between -π and π in a symbol duration). In an optical QPSK symbol, overlaps between adjacent symbols can result in inter-symbol interference, which further increases the scrambling effect for the optical signal.

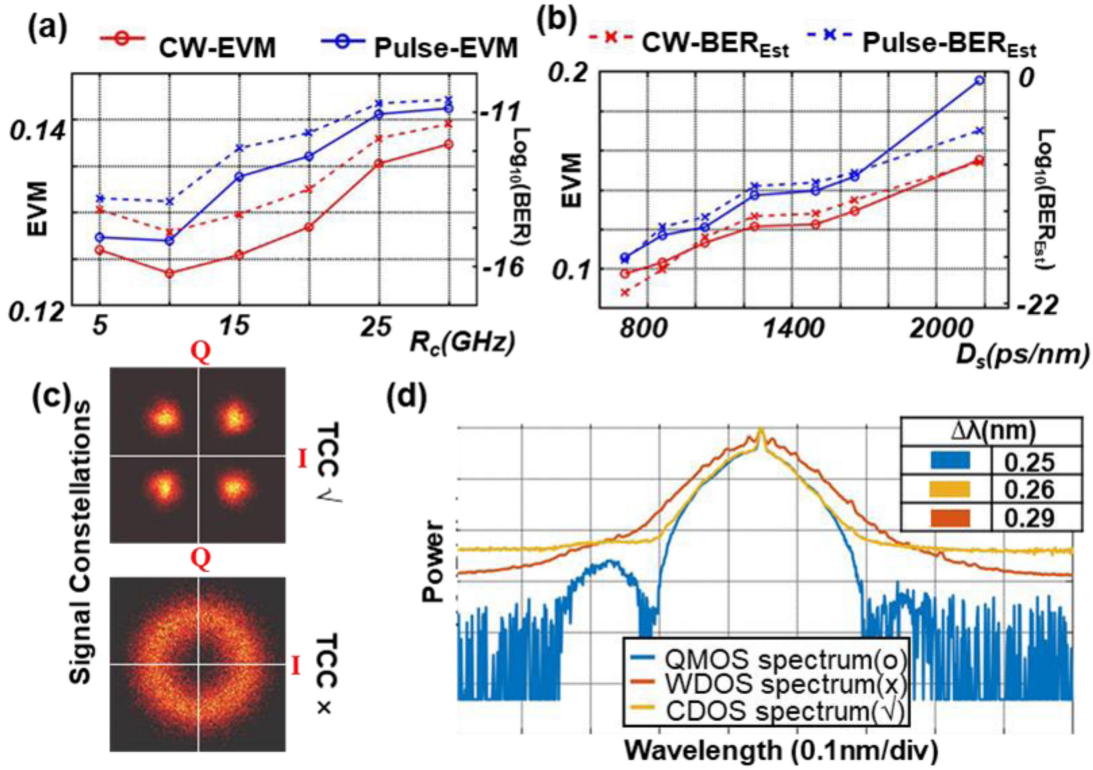

Fig. 6. (a)&(b) The **EVM** and $\mathbf{BER_{Est}}$ curves for B2B system with different $\mathbf{R_c}$ and $\mathbf{D_s}$. (c) signal constellations for CDOS (√) and WDOS (×) in the transmission through the classical channel (TCC). (d) The optical spectra and bandwidths for the QPSK modulated optical signal (QMOS), WDOS, and CDOS.

B. Transmission Property

Fig. 6 shows the transmission results in the experiment. The systems performance using both CW and an externally pulsed laser source are plotted in this figure. The error vector magnitude (**EVM**) and bit error rate (BER) were used to measure the quality of the recovered QPSK signal, where the **EVM** is a figure of merit normally used to quantify the performance of M-ary PSK or QAM signals [24]–[26]. Fig. 6(a)&(b) are the transmission performance of the back-to-back (B2B) system with the variables of $\mathbf{R_c}$ and $\mathbf{D_s}$. The BER ($\mathbf{BER_{Est}}$) was estimated from the **EVM** by [26]:

$$\mathbf{BER_{Est}} = \frac{2\mathbf{k}\left(1-1/\sqrt{\mathbf{M}}\right)}{\log_2 \mathbf{M}}\ \mathrm{erfc}\left[\sqrt{\frac{3/2}{(\mathbf{M}-1)\,\mathbf{EVM}^2}}\right] \tag{6}$$

where $\mathbf{k} = 2.9$ is a correction factor for the QPSK system and $\mathrm{erfc}[\cdot]$ is the complementary error function.

From the experimental results for the system's transmission in Fig. 6(a), the **EVM** for the B2B systems with different $\mathbf{R_c}$ were lower than 15%. When the TDSPE components and transmission fiber were removed as a comparison, the **EVM** and $\mathbf{BER_{Est}}$ for a classical QPSK system were 9.75% and −23.7 respectively. The fluctuation in the $\mathbf{R_c}$ curves might be caused by a timing mismatch in the system's synchronization which was shorter than the minimal adjustment resolution of the delay lines (∼5 ps). The requirement for synchronization accuracy became increasingly significant with the growth of $\mathbf{R_c}$, which accounts for the slight increase of the **EVM** curves. The logarithmic $\mathbf{BER_{Est}}$ curves exhibited the same trend as the **EVM** curves. Both logarithmic $\mathbf{BER_{Est}}$ curves were lower than −10 and this indicated that the growth of $\mathbf{R_c}$ had less effect on the system transmission performance and the operation of TDSPE is independent of the data transmission. The gap between the CW laser curve and pulsed laser curve were caused by the signal attenuation in the intensity modulation. However, the attenuation effect in the DCF was critical for the transmission property. For example, the **EVM**s for both cases were lower than 12% at $\mathbf{D_s} = -706$ ps/nm while the **EVM** would raise to 19.65% and 15.54% for the pulsed and CW carrier respectively when $\mathbf{D_s}$ reaches −2178 ps/nm. The corresponding logarithmic $\mathbf{BER_{Est}}$ curve were increasing from −23 to −9. This phenomenon was also obvious in the security investigation shown in Fig. 7. As a solution, using a highly dispersive element with lower loss and a nonlinear effect, such as a linear chirped fiber Bragg grating, could effectively eliminate this phenomenon. When transmitting through the SMF, the signal's attenuation and the noise introduced by the amplifier would increase the **EVM** as well. By comparing the curves in Fig. 6(a)&(b), it can be seen that applying the TDSPE has less influence on the transmission performance, except a certain power loss is introduced, which depends on the devices serving for TDSPE.

Fig. 6(c) depicts signal constellation diagrams for CDOS (√) / WDOS (x) in the system with the transmission through the classical channel (TCC). As a compromise for the overall system performance, the transmitted frame length was 65536 bits.

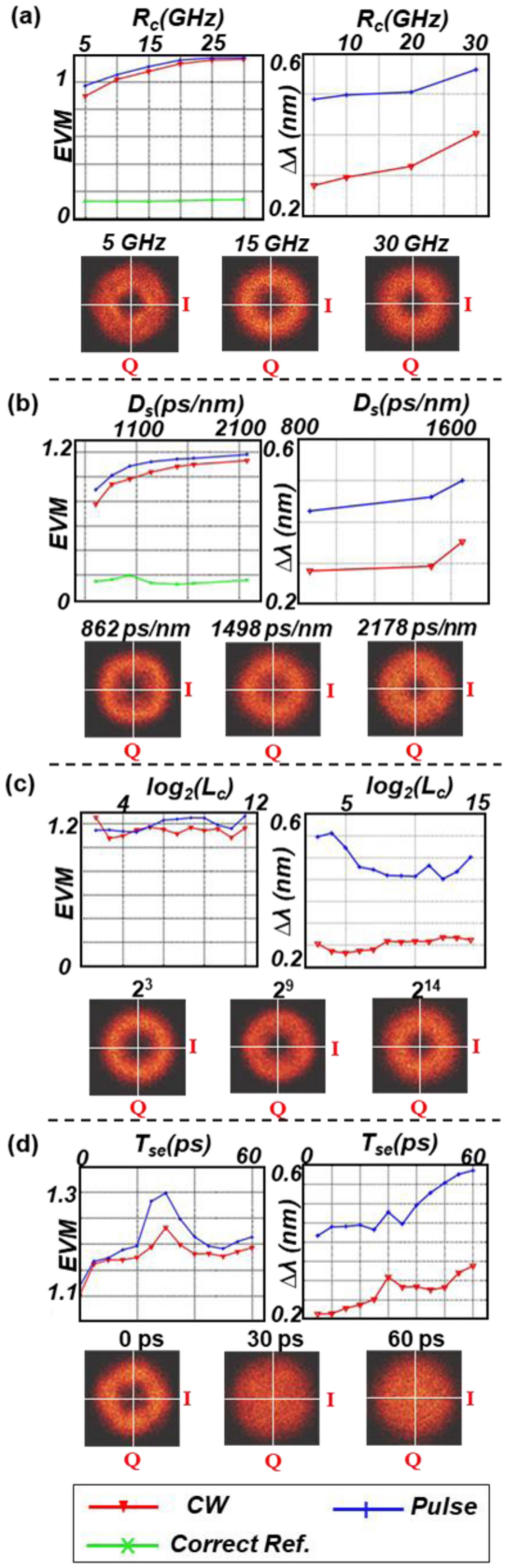

Fig. 7. The performance of the QKD seeded TDSPE QPSK system, with the signal constellation diagrams shown below, for different SC rates ($\mathbf{R_c}$), total stretching dispersions ($\mathbf{D_s}$), SC lengths ($\mathbf{L_c}$), and timing synchronization errors ($\mathbf{T_{se}}$) investigation.

Therefore, the lowest measurable BER ($\mathbf{BER_{Mea}}$) was $\sim 1.5 \times 10^{-5}$ (logarithmic $\mathrm{BER_{Mea}} \approx -4.5$). From the experimental results, no error was detected in both B2B and TCC systems (Fig. 6 (a)-(c)), which meant that the measured logarithmic BER ($\mathrm{BER_{Mea}}$) was less than -4.5. From Fig. 6(c), the measured **EVM** for the CDOS / WDOS were 20.31% and 115.87% respectively, which correspond to the logarithmic $\mathbf{BER_{Est}}$ of -5.90 and -0.25. The information entropy was around 2.43×10^{-5} and 0.47. This indicates that integrated security scheme was sufficient to scramble the transmitted data in the TCC system.

Fig. 6(d) shows the optical spectra for the QPSK signal, WDOS, and CDOS. The inset shows the measured 20-dB bandwidth of the three signals, which were 0.25, 0.26, and 0.29 nm, respectively. An obvious spectral extension could be found in the encoded optical signal compared with the QPSK signal and CDOS. This is mainly caused by the code scrambling and overlapping effect of the TDSPE. The spectral extension for the CDOS was mainly caused by the unbalanced phase modulation depth and the timing mismatch.

C. Scrambling Effect

Theoretically, there is less effect on the encoding performance if $\mathbf{L_d}$ is filled by repeating a short code. But, from the discussion in Section V, $\mathbf{N_k}$ is a critical parameter in determining the probability of successful eavesdropping. Although the synchronization header is public for detection in the data frame, it is still likely to exist the synchronization timing error [11] ($\mathbf{T_{se}}$) between the transmitter (Alice) and receivers (Bob, and Eve). When the synchronization timing error exists in the decoded optical signal, the process of spectral phase encoding generates ultra-short mismatch chips, which contains ultra-high frequency components, in the optical signal. Therefore, the $\mathbf{N_k}$ and $\mathbf{T_{se}}$ were also considered in the system security performance together with $\mathbf{D_s}$ and $\mathbf{R_c}$.

The **EVM** curves and signal diagrams with different SC rate $\mathbf{R_c}$, stretching dispersion $\mathbf{D_s}$, SC length $\mathbf{L_c}$, and synchronization timing error $\mathbf{T_{se}}$ are shown in Fig. 7 to investigate the security performance of the system. For comparison purposes, the system performance for the externally pulsed laser source is also shown in this figure together with the results for CW source. 20 dB bandwidth of the signal spectra ($\Delta\lambda$) was used to evaluate the scrambling effect in the spectral domain. Higher **EVM** value and larger bandwidth indicate greater TDSPE scrambling effect, and therefore higher security performance.

The experimental results shown in Fig. 7 verified that the growth of $\mathbf{R_c}$ and $\mathbf{D_s}$ would result in an obvious increase of the **EVM** and bandwidth. It can be seen from the signal constellation diagrams that, the recovered WDOS was scrambled to some extent when the low $\mathbf{R_c}$ and $\mathbf{D_s}$ were applied, but it could also be observed that the recovered signal converged to the four referenced QPSK states. When the $\mathbf{R_c}$ and $\mathbf{D_s}$ increased to a high value (e.g. 30 GHz and 2178 ps/nm respectively), the scrambled signals would randomly locate at an annulus. The transmitted QPSK states were well hidden in the noise-like signal distribution.

It is important to notice that the higher $\mathbf{D_s}$ would introduce more signal loss, because the increase of the stretching dispersion was performed by using a longer DCF. In the curve for $\mathbf{D_s}$, the slight raise of the **EVM**s in the CDOS implied the deterioration of the OSNR caused by the DCF. However, in the experiment, both Erbium-doped fiber amplifiers (EDFAs) were operating in the 'power control' mode. Their output signal power was constant, so the growth of the **EVM** caused by the DCF was small enough to be neglected for the scrambling effect study.

In the investigation for the $\mathbf{L_c}$, it was varied from 2^3 to 2^{14} in the experiment to evaluate the scrambling effect, where a short SC ($\mathbf{L_c}$) was repeated to fill $\mathbf{L_d}$ to mask the whole data frame. From Fig. 7, there was no difference observed in the scrambling effect with different vales of $\mathbf{L_c}$, which indicated that the $\mathbf{L_c}$ and key refresh rate has less effect on the scrambling effect of TDSPE. As a result, they could be a variable to improve the flexibility of the system and effectively increase the time required for the SC testing (which will be introduced in Section V). The results in the security analysis also suggest that $\mathbf{L_c}$ was negatively correlated with the probability of the successful attack. Consequently, longer sequences can be used in the scrambling process without negative impact on the system transmission performance figures of merit.

When analysing the results of $\mathbf{T_{se}}$, a further scrambling effect could be observed based on the wrongly decoded case with the $\mathbf{D_s}$ of 1498 ps/nm. An offset, growing with the increase of $\mathbf{T_{se}}$, existed in both **EVM** and bandwidth curves. This was caused by the loss of the optical delay line that was used for synchronization. The higher delay would suffer more power loss. As there was no power compensation after the optical delay line, this part of loss directly impacted the detection performance. Ignoring this offset, the scrambling effect in both time and spectral domain reached their peak at 30 ps, because 30 ps equalled to $\mathbf{T_c}$/2, and the signal spectrum had the most effective scrambling caused by $\mathbf{T_{se}}$ at this point. As the experimental system had the overall response bandwidth of 20 GHz, the ultra-high frequency component of WDOS was filtered. From Fig. 6 and Fig. 7(d), it can be concluded that the system's tolerance for the synchronisation error was between 5 ps to 10 ps. The $\mathbf{T_{se}}$ is a common problem for the receivers (Bob and Eve) in the proposed security scheme. But Eve must deal with the code scrambling, overlapping scrambling, and synchronization timing error simultaneously.

As a comparison, the scrambling effect of the externally pulsed laser, with different scrambling factors, is also illustrated in Fig. 7. The **EVM** and bandwidth for the CDOS pulsed laser were 17.96% and 0.38 nm, respectively. For the security investigation, the pulsed laser had a similar trend to the CW laser case in both time and spectral domains. But, in the low $\mathbf{R_c}$ and $\mathbf{D_s}$ cases (e.g. 5 GHz and 862 ps/nm), the externally pulsed laser could partly enhance the system's security, because of its larger bandwidth. At the high value for $\mathbf{R_c}$ and $\mathbf{D_s}$, the scrambling effect caused by the higher frequency was less functional. Thus, the two **EVM** curves became closer to each other with the increase of $\mathbf{R_c}$ and $\mathbf{D_s}$.

V. Security Analysis for Classical Channel

In this work, eavesdroppers are assumed to have full knowledge of the entire system configuration except for SC (generated by the QKD system and therefore inheriting all of the security guarantees provided by that system). The brute-force attack is studied in this paper only.

Eavesdropping of the classical channel (where the transmitted signal is scrambled by the TDSPE scheme) through a brute-force attack would require Eve to be capable of generating sufficient copies of the optical signal, so that she can test all possible SC patterns by using them to decode the optical signal copies, and convert the decoded optical signal to electrical signals by photodetectors, where this process is called 'SC testing'. Successful eavesdropping would require performing the SC testing in real time to convert the correctly decoded optical signal into the electrical domain for further signal processing before the optical signal dissipates in the medium (as the optical signal could not be stored in the same manner as the detected electrical signal). If Eve could not perform the real-time SC testing, the optical signal would be incorrectly decoded, and the converted electrical signal would have a noise-like performance which was discussed in Section IV. Since the optical signal is no longer available after optical-to-electrical converters, Eve will not be able to recover the original data and has lost the information forever.

As the SC is protected by the QKD system, Eve lacks the knowledge of SC and requires enough optical signal copies to complete the SC testing. As the length of the SC for encoding a data frame is $\mathbf{L_d}$, there are $2^{\mathbf{L_d}}$ possible SC patterns in the data frame. Eve would need to generate $2^{\mathbf{L_d}}$ copies of the optical signal in real time for the SC testing. Fig. 8 shows a schematic diagram of an idealized brute-force eavesdropping attack model (real-time SC testing). To briefly describe the theoretical ability of copying the optical signal, two simplified signal copying models are considered here: optical-signal splitting (green region of Fig. 8) and time-domain copying (orange region of Fig. 8), where they are assumed to copy the signal launched from the demo system (shown in Fig. 4).

The optical-signal splitting model, shown in the green region of Fig. 8 consists of a serial of cascaded optical power splitting layers. Each splitter layer is followed by optical signal amplifiers to maintain the optical power level above the minimum level for further signal splitting/amplification/detection in the next layer. However, this process will result in deterioration of the SNR as the amplification will introduce extra noise. Assuming that the optical signal is equally split at each layer, and all amplifiers have the same gain $\mathbf{G}$ and noise figure $\mathbf{F_G}$. Thus, the total noise figure ($\mathbf{F}$) [27] in this model can be expressed as:

$$\mathbf{F} = \mathbf{F_G} + \sum_{\mathbf{n}=1}^{\mathbf{N}} \frac{\mathbf{F_G}}{\prod_{\mathbf{m}=1}^{\mathbf{n}} \mathbf{L_m G^{n+1}}} \tag{7}$$

where $\mathbf{N}$ is the total number of splitting layers.

Under this model, the production of new optical signal copies will not be available for the further recovery when the SNR of the split signal is reduced to the minimum level ($\mathbf{SNR_{min}}$). For

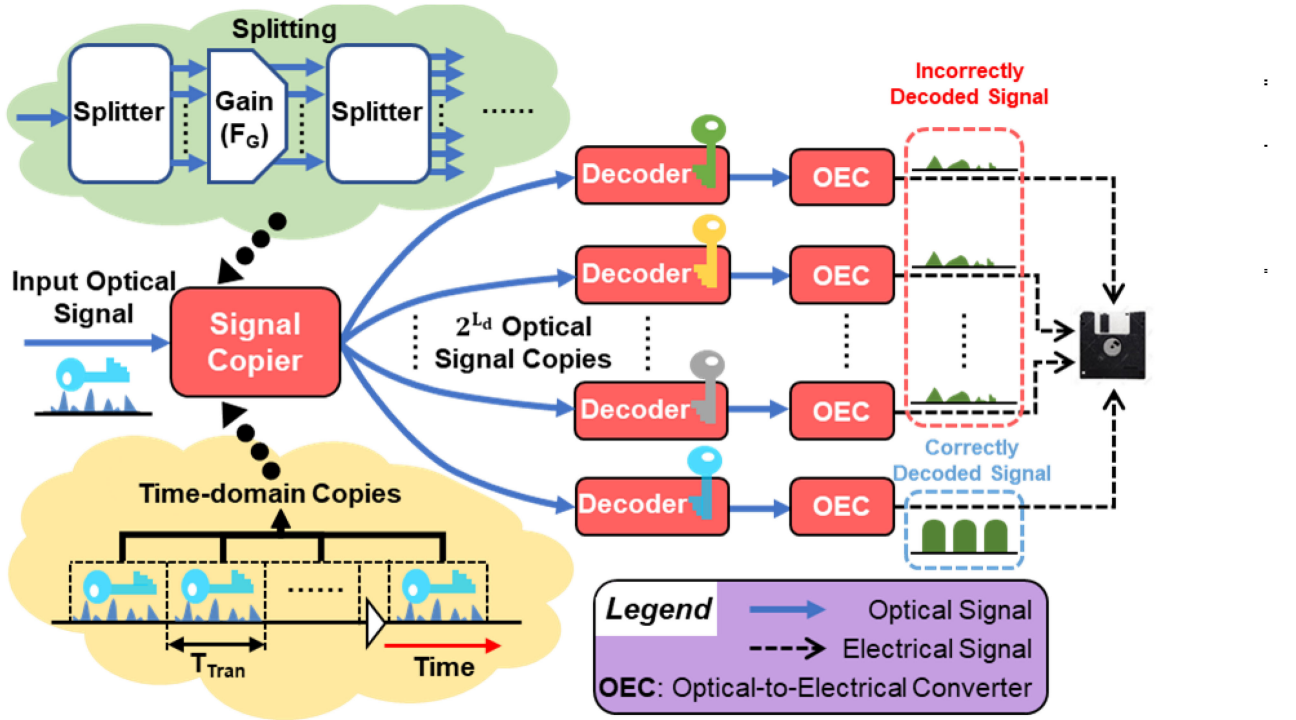

Fig. 8. Schematic diagram of Brute-force Eavesdropping attack model. The green and orange 'cloud' regions respectively indicate separate possible simplified signal copying models that could reside within the red 'Signal Copier' box.

TABLE I
SECURITY ANALYSIS RESULTS FOR THE MODELS

Model	Maximum Number of Copies (C)	Probability for the successful attack (P)
Splitting	2.7×10^{828}	3.1×10^{-7398}
Time-domain copying	1.1×10^{5}	1.2×10^{-8221}

QPSK modulation, $\mathbf{SNR_{min}}$ is around 2 dB [28]. Therefore, the maximum number of the signal copies (**C**) that could be generated in this theoretical model is limited by the total noise figure (**F**). In Table I, it can be seen that $\mathbf{C}\approx 2.7\times10^{828}$ when $\mathbf{F}\approx$ 24.75 dB. Comparing to the total number of possible SC patterns (2^{27326}), the possibility for a successful attack is infinitely small (3.1×10^{-7398}). Therefore, the use of a brute-force approach to successfully decode the signal is impossible in practical terms, assuming no *a priori* knowledge of the encryption key.

Another idealized model is the time-domain copying model, shown in the orange region of Fig. 8 Assuming that standard 9 μm core diameter telecommunications optical fiber is used as the optical delay medium, optical signal amplifiers are needed to compensate for the fiber losses. These amplifiers introduce extra noise to the signal copies, and the optical signal can be ideally duplicated in the time domain within the duration of the optical delay. Similar to that in the splitting model, the maximum number of signal copies **C** is limited by the deterioration of the SNR and is around 1.1×10^{5} when fiber conforming to the G.652 standard is used to generate the optical delay. This is much less than the splitting model. The possibility of a successful brute-force attack is practically impossible ($P \approx 1.2 \times 10^{-8221}$) in this model. Even if the SNR deterioration was further ignored, in order to generate 2^{27326} optical signal copies for the SC testing, there would be a requirement to retain the optical signal for more than 4.9×10^{8212} years. This is practically impossible with known current technology.

It is worth noting that if the generated SC is too short, the number of the possible SC patterns would decrease exponentially, and the data becomes vulnerable to the brute-force attack. In general, the longer the length of SC the stronger the security of the system against brute-force attacks.

From the above discussion, we can conclude that, in the proposed system, the eavesdropper would need to perform real-time SC testing to attack the security of the system. Such an eavesdropping attack would require enormous resources and the success probability is negligible. Once the real-time brute-force attack has failed, the optical signal will be attenuated in the medium and the eavesdropper will not be able to record and recover the information in the electrical domain. The system security performance for the case that the scrambled optical signal is converted into an electrical signal without the correct decoding was investigated by numerical simulation and experimental results in Section IV.

VI. CONCLUSION

We have demonstrated an encrypted 40 Gbps communication scheme over 52.3 km using TDSPE with the encryption and decryption keys being securely shared between transmitter and

receiver using quantum key distribution. The TDSPE operates with coherent QPSK modulation using CW laser source. 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 quantum key. Meanwhile, the security performance with different security factors were also investigated. And it suggested that the larger stretching dispersion value, higher encoding rate, longer scrambling code, or higher symbol rate could improve the security performance. Since the key distribution was carried out prior to the TDSPE and data transmission, the integration of QKD and TDSPE is potential to be further designed for real-time operation. The proposed integrated "Plug and play" security module could be further applied to practical high-speed optical transmission systems with higher data rates, higher order modulations (such as 16QAM/64QAM), and polarization-division multiplexing.

ACKNOWLEDGMENT

The author Kexin Wang would like to thank Dr. Hongliang Guo for his help with the eavesdropping models.

REFERENCES

[1] A. Biryukov and D. Khovratovich, "Related-key cryptanalysis of the full AES-192 and AES-256," in *Proc. Adv. Cryptol.*, Berlin, Heidelberg, M. Matsui, Ed., 2009, vol. 5912, pp. 1–18.
[2] H.-K. Lo, M. Curty, and K. Tamaki, "Secure quantum key distribution," *Nature Photon.*, vol. 8, pp. 595–604, 2014.
[3] B. Korzh *et al.*, "Provably secure and practical quantum key distribution over 307 km of optical fibre," *Nature Photon.*, vol. 9, pp. 163–168, 2015.
[4] L. C. Comandar *et al.*, "Room temperature single-photon detectors for high bit rate quantum key distribution," *Appl. Phys. Lett.*, vol. 104, no. 2, 2014, Art. no. 021101.
[5] X. Tang, A. Wonfor, R. Kumar, R. V. Penty, and I. H. White, "Quantum-safe metro network with low-latency reconfigurable quantum key distribution," *J. Lightw. Technol.*, vol. 36, no. 22, pp. 5230–5236, 2018.
[6] P. J. Clarke, R. J. Collins, P. A. Hiskett, P. D. Townsend, and G. S. Buller, "Robust gigahertz fiber quantum key distribution," *Appl. Phys. Lett.*, vol. 98, no. 13, 2011, Art. no. 131103.
[7] I. Quantique. *Clavis300 quantum cryptography platform*, ID Quantique SA, 2019, Accessed: Apr. 18, 2020, [Online]. Available: https://marketing.idquantique.com/acton/attachment/11868/f-42e4a1b3-46a2-4f2f-8fcd-ba9118954c3a/1/-691 /-/-/-/Clavis300_QKD_Brochure.pdf
[8] A. Aguado *et al.*, "Hybrid conventional and quantum security for software defined and virtualized networks," *IEEE/OSA J. Opt. Commun. Netw.*, vol. 9, no. 10, pp. 819–825, Oct. 2017.
[9] X. Wang and N. Wada, "Spectral phase encoding of ultra-short optical pulse in time domain for OCDMA application," *Opt. Exp.*, vol. 15, no. 12, 2007, Art. no. 7319.
[10] X. Wang, Z. Gao, X. Wang, N. Kataoka, and N. Wada, "Bit-by-bit optical code scrambling technique for secure optical communication," *Opt. Exp.*, vol. 19, no. 4, 2011, Art. no. 3503.
[11] Z. Gao, B. Dai, X. Wang, N. Kataoka, and N. Wada, "Rapid programmable/code-length-variable, time-domain bit-by-bit code shifting for high-speed secure optical communication," *Opt. Lett.*, vol. 36, no. 9, 2011, Art. no. 1623.
[12] Z. Gao, B. Dai, X. Wang, N. Kataoka, and N. Wada, "10-Gbit/s, reconfigurable time domain SPE-OCDMA system with code shifting and pulse overlapping," *Microw. Opt. Technol. Lett.*, vol. 54, no. 3, pp. 808–810, 2012.
[13] Z. Gao, B. Dai, X. Wang, N. Kataoka, and N. Wada, "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," *Opt. Lett.*, vol. 36, no. 22, 2011, Art. no. 4326.
[14] B. Dai, Y. Huang, Z. Jiao, K. Wang, D. Zhang, and X. Wang, "Confidentiality analysis of optical code-based secure optical communication system," *Opt. Eng.*, vol. 57, no. 10, 2018, Art. no. 100502.
[15] *Information technology — Open Systems Interconnection — Basic Reference Model: Naming and addressing*, ISO/IEC 7498-3:1997, 1997.
[16] X. Zhou, R. Urata, and H. Liu, "Beyond 1 Tb/s intra-data center interconnect technology: IM-DD OR coherent?," *J. Lightw. Technol.*, vol. 38, no. 2, pp. 475–484, Jan. 2020.
[17] S. J. Savory, "Digital coherent optical receivers: Algorithms and subsystems," *IEEE J. Sel. Topics Quantum Electron.*, vol. 16, no. 5, pp. 1164–1179, May 2010.
[18] J. F. Dynes *et al.*, "Cambridge quantum network," *npj Quantum Inf.*, vol. 5, no. 1, 2019, Art. no. 101.
[19] T. Xu *et al.*, "Chromatic dispersion compensation in coherent transmission system using digital filters," *Opt. Exp.*, vol. 18, no. 15, 2010, Art. no. 16243.
[20] M. Lucamarini *et al.*, "Efficient decoy-state quantum key distribution with quantified security," *Opt. Exp.*, vol. 21, no. 21, pp. 24550–24565, 2013.
[21] A. Shields, "Core and access QKD networks," in *Proc. 7th Int. Conf. Quantum Cryptogr.*, Cambridge, UK, Sep. 18, 2017, vol. QCrypt2017, Art. no. Tu11.
[22] "Toshiba QKD system," 2019. Accessed: Oct. 18, 2019. [Online]. Available: https://www.toshiba.eu/eu/Cambridge-Research-Laboratory/Quantum-Information/Quantum-Key-Distribution/Toshiba-QKD-system/
[23] G. Brassard and L. Salvail, "Secret-key reconciliation by public discussion," in *Proc. Adv. Cryptol.*, Berlin, Heidelberg, T. Helleseth, Ed., 1994, pp. 410–423.
[24] H. Qin and X. Xiao, "Effects of fiber nonlinearity on error vector magnitude and bit error ratio for advanced modulation formats," *Opt. Eng.*, vol. 57, no. 5, 2018, Art. no. 056101.
[25] R. Schmogrow *et al.*, "Error vector magnitude as a performance measure for advanced modulation formats," *IEEE Photon. Technol. Lett.*, vol. 24, no. 1, pp. 61–63, Jan. 2012.
[26] I. Fatadin, "Estimation of BER from error vector magnitude for optical coherent systems," *Photon. J.*, vol. 3 2016, Art. no. 21.
[27] D. M. Baney, P. Gallion, and R. S. Tucker, "Theory and measurement techniques for the noise figure of optical amplifiers," *Opt. Fiber Technol.*, vol. 6, no. 2, pp. 122–154, Apr. 2000.
[28] A. D. Ellis, M. E. McCarthy, M. A. Z. Al Khateeb, M. Sorokina, and N. J. Doran, "Performance limits in optical communications due to fiber nonlinearity," *Adv. Opt. Photon.*, vol. 9, no. 3, pp. 429–503, 2017.

Kexin Wang received the B.S. degree from the Beijing University of Posts and Telecommunications, Beijing, China, in 2015, and the M.S. degree in 2017 from Heriot-Watt University, Edinburgh, U.K., where he is currently working toward the Ph.D. degree with the Advanced Optical Communication and Imaging Lab, Institute of Photonics and Quantum Sciences. His research interests include high-speed secure optical communication systems, optical layer security, underwater optical wireless communication, and 3D printing techniques.

Xinke Tang received the M.Res. and Ph.D. degrees from the University of Cambridge, Cambridge, U.K., in 2014 and 2019, respectively. He is currently a Research Assistant Professor with Peng Cheng Laboratory, Shenzhen, China. His research interests include underwater optical wireless communication, optical networks, optical switching, and quantum key distribution.

Adrian Wonfor (Member, IEEE) biography not available at the time of publication.

Robert John Collins (Member, IEEE) received the M.Phys. (Hons.) degree in physics from Heriot-Watt University, Edinburgh, U.K., in 2004 and the Ph.D. degree in physics under the supervision of Prof. Gerald S. Buller from Heriot-Watt University, in 2008. He was a Postdoctoral Research Associate with the Single-Photon Group (headed by Prof. Gerald S. Buller), Institute of Photonics and Quantum Sciences, Heriot-Watt University. While at Heriot-Watt University, his research interests included quantum communications and related technologies. He has been a Member of the UK Institute of Physics since 1999, Optical Society of America since 2010, SPIE since 2010, and a Charter Physicist since 2021.

Gerald S. Buller is currently a Professor of physics with Heriot-Watt University, Edinburgh, U.K. In 2002, he Co-Founded Helia Photonics, and is currently the company Chairman. His research interests mainly include associated with photon-counting technology and applications, including quantum communications, quantum imaging, time-of-flight ranging, and imaging. He is a Fellow of the Optical Society of America, Institute of Physics (UK), and Royal Society of Edinburgh. In 2015, he was awarded the EPSRC Established Career Fellowship in Quantum Technology.

Richard V. Penty (Senior Member, IEEE) received the Ph.D. degree in engineering from the University of Cambridge, Cambridge, U.K., in 1989. He is currently a Professor of photonics with the University of Cambridge, having previously held academic posts with the University of Bath, Bath, U.K., and the University of Bristol, Bristol, U.K. He has authored more than 900 refereed journal and conference papers. His research focuses on optical fiber devices for signal processing applications, where he was a Science and Engineering Research Council Information Technology Fellow researching on all optical nonlinearities in waveguide devices. His research interests include high speed optical communication systems, photonic integration, optical switching, and sensing systems. He is also Deputy Head of the School of Technology and a Deputy Vice Chancellor with the University of Cambridge and Master of Sidney Sussex College. He is a Fellow of the Royal Academy of Engineering and the IET.

Ian H. White (Fellow, IEEE) took up his role as the Vice-Chancellor of the University of Bath, Bath, U.K., in April 2019. He had previously been Master of Jesus College, University of Cambridge, Cambridge, U.K. He is a Co-Founder of Zinwave Ltd., a company providing wireless coverage solutions, and PervasID Ltd., which develops ultra-high-frequency RFID readers. He has authored or coauthored more than 1000 papers and more than 30 patents. His research interests include photonics, including optical data communications and laser diode-based devices. He is a Fellow of the Royal Academy of Engineering, the Institute of Electrical and Electronic Engineers, and the Institution of Engineering and Technology.

Xu Wang (Senior Member, IEEE) received the Ph.D. degree in electronics engineering from the Chinese University of Hong Kong, Hong Kong, in 2001. He is with the National Key Laboratory of Fiber Optic Broad-band Transmission and Communication Networks, UESTC, China, the Department of Electronic Engineering, CUHK, Department of Electronic and Information Systems, Osaka University, Osaka, Japan, Photonic Network Group of National Institute of Communication and Information Technology, Tokyo, Japan. He is currently an Associate Professor with the Institute of Photonics and Quantum Sciences, Heriot-Watt University, Edinburgh, U.K. He leads the Advanced Optical Communication and Imaging Lab, Heriot-Watt University. His research interests include high-speed optical communication, optical signal processing, and ultrafast imaging.