IEEE Transactions on Quantum Engineering

Received 8 July 2024; revised 10 November 2024; accepted 20 November 2024; date of publication 27 November 2024; date of current version 17 December 2024.

Digital Object Identifier 10.1109/TQE.2024.3507155

FPGA-Based Synchronization of Frequency-Domain Interferometer for QKD

NISHANTH CHANDRA AND PRADEEP KUMAR KRISHNAMURTHY

Department of Electrical Engineering, Indian Institute of Technology, Kanpur 208016, India

Corresponding author: Nishanth Chandra (e-mail: nishc@iitk.ac.in).

This work was supported by the Department of Science and Technology India under Grant DST/ICPS/Theme-1/2019.

ABSTRACT In this article, we propose and experimentally demonstrate a novel synchronization method for quantum key distribution (QKD) systems. The method consists of maximizing the visibility of frequency-domain interference of optical sidebands about an optical carrier at the receiver node. The sidebands are generated by phase modulation of the optical carrier by an radio-frequency (RF) signal whose phase can be dynamically varied. The phase-variable RF signal is generated by the field-programmable gate array (FPGA) at the transmitter and the receiver using GTX transceivers. In order to facilitate this, we use square waveforms for RF signal instead of the conventional sinusoidal signals. We derive mathematical expressions for sideband power as a function of the phase difference between RF signals at transmitter and receiver. The phase is adjusted using dynamic phase shifter module, implemented by the FPGA. We propose a complete workflow that allows transmitter and receiver synchronization to within 12.6 ps directly over the quantum channel of QKD systems. Once synchronized, the same system can be switched over to quantum transmission by user-defined time delay. The workflow was implemented on a Xilinx Kintex-7 KC705 FPGA board. We studied the robustness of our technique by evaluating the stability of the interferometer over an operation of 10 min with standard deviation of interference to be less than 9% of the mean detection amplitude.

INDEX TERMS Clock synchronization, field-programmable gate array (FPGA), frequency-coded quantum key distribution (FC-QKD), GTX transceiver, quantum communication, quantum cryptography, quantum key distribution (QKD).

I. INTRODUCTION

Synchronization is critical in many applications, such as communication links, frequency and time transfer, nuclear experiments, medical diagnostics, etc. [1], [2], [3]. In communication links, synchronized clocks provide a common measure of time to communicating parties ensuring that the receiver samples the received signals at right instants of time. Clock synchronization is also essential for identifying the start of frame of the message. In quantum communications, information of the time of arrival of photon pulse is essential for gating the single-photon detector (SPD) at the receiver [4]. The requirement of precise clock synchronization becomes more stringent in the case of frequency-coded quantum key distribution (FC-QKD) systems [5].

In the discrete-variable FC-QKD, Alice encodes random bits in the phase values of the radio-frequency (RF) signal, which is then used to modulate the optical carrier. This modulation generates sidebands around the optical carrier from which qubits are formed. The average photon number in the sideband is kept less than 1 to approximate a single-photon source for QKD applications. At the receiver, Bob again modulates the received photons with the RF signal of the same frequency, but with independent random phases, causing interference in the optical sideband. The interference result that depends on the phase difference between Alice and Bob's RF signals establishes the private secret key bits between Alice and Bob. This system requires the RF carriers at Alice and Bob's ends to be frequency and phase locked. Any synchronization error amounts to reduced interference visibility, which translates into intrinsic quantum bit error rate [6].

Various techniques of clock synchronization are employed in QKD. Synchronization schemes for finding the optimized gating window of SPDs are discussed in [7] and [8]. In [9], [10], and [11], clock for synchronization is derived from an external reference, such as GPS, Global Navigation

Satellite System, or NavIC. In [12] and [13], a decimated clock is transmitted through a separate synchronization channel, either through a separate fiber, or multiplexing over the same fiber, which is also used for quantum channel on a different wavelength [14], [15]. Shakhovoy et al. [16] proposed to further simplify the optical setup by using the same laser to generate synchronization and quantum signals at different wavelengths through pump current variation. The studies in [17], [18], and [19] discuss qubit-based synchronization methods wherein the synchronization is performed after the quantum communication before postprocessing, and is extended to synchronize the multiuser quantum access networks in [20]. Synchronization precision achieved in these methods is limited by the inherent jitter from the SPDs that are employed [21]. However, phase locking of the high-frequency RF signals in FC-QKD requires synchronization to be less than SPD jitter. In this work, we have explored field programmable gate arrays (FPGAs) for higher precision synchronization in the FC-QKD systems.

FPGA-based time-to-digital converters (TDCs) have been explored for the purpose of high-precision synchronization. The high precision in these TDCs is achieved using chain of delay elements in the FPGAs called tapped delay lines [22], [23]. Polarization-coded QKD applications use carry chains as tapped delay lines for time interval analyzer [24], [25]. An improved design makes use of large-scale multiphase matrix (LSPM) [26], [27]. These techniques make use of the picosecond scale delays introduced by the logic cells inside the FPGAs. Precision upto 1 ps is reported using these state-of-the-art FPGA technologies. However, we note that all the logic cells of the delay line do not provide equal delay. Furthermore, the propagation delay of the logic cells is a function of temperature and power supply voltage. Thus, these techniques require frequent calibration of each delay cell and stored in the FPGA internal memory [28]. In this article, we use the dynamic phase shifting feature of the multimode clock manager (MMCM) block of the FPGA. This ensures a deterministic delay of 12.6 ps for Kintex-7 series FPGAs. A resolution of 12.6 ps causes a visibility loss of less than 0.5%, as will be shown in Section II. The advantage of our approach is that it avoids using large arrays of logic cells for tapping delays, reducing the circuit complexity and lower device utilization. Lower utilization of FPGA resources becomes important as other QKD modules, such as postprocessing, also need to be implemented on the same FPGA [29], [30], [31]. For example, the lookup table (LUT) resource utilization of postprocessing modules implemented on Xilinx Virtex-6 LX240T FPGA was reported as high as 42% [32].

All the previous implementations of FC-QKD use a sinusoidal RF signal to modulate the optical carrier [5], [14], [15], [33], [34], [35], [36]. Such RF signals are generated using VCOs and phase-locked loop (PLLs), which also require a decimated frequency sinusoidal clock for synchronization at the receiver end [36]. In this article, we generate the RF signal using the FPGA GTX transceiver, which outputs a square waveform. The transceiver uses a square waveform as clock input. Such a scheme simplifies the RF subsystem of FC-QKD. It also allows for easy reconfiguration of the QKD system for various protocols, such as BB84 or B92. Further, the RF frequency of operation and bit-rate can also be modified without any change in hardware. The ability to reconfigure bit-rate in the runtime would allow to adaptively change the repetition rate of the single-photon detection based on the current conditions of the dark count, thus contributing toward increasing the key rate.

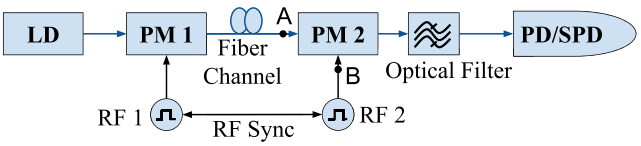


FIGURE 1. Conceptual block diagram of FC-QKD system. Laser diode (LD), optical phase modulator (PM), photodetector (PD), and single-photon detector (SPD).

In this article, we discuss the circuit implementation of various modules required for QKD applications and also for synchronization applications in other possible areas. The rest of this article is organized as follows. Section II discusses the theory of frequency-domain interference using cascaded electro-optical phase modulators, and the principle of FC-QKD. We present the experimental setup of FPGA-based frequency-domain interferometer, along with detailed circuits of the FPGA modules in Section III. In Section IV, we present the workflow for initialization, handshaking, synchronization, and quantum communication, followed by discussion in Section V. Finally, Section VI concludes this article.

II. THEORY OF OPERATION

A. MATHEMATICAL DESCRIPTION

In this section, we discuss and obtain expressions for frequency-domain sideband interference with square RF waveform for synchronization. Fig. 1 shows the conceptual block diagram of FC-QKD system. In the quantum transmission phase, the photodetector will be replaced by SPDs to record the qubits. Considering the classical mode of operation, for illustrating the synchronization phase, the electric field of the optical signal emitted by the laser diode LD is phase modulated by a square wave RF signal using the optical phase modulator PM1. The electric field at the output of PM1 can be written as

$$E_1(t) = E_{\text{in}}(t) \exp\left(j \frac{\pi u_1(t)}{V_\pi}\right) \tag{1}$$

where E_{in} is the electric field of the optical carrier, given by $E_0 \exp(j\omega_0 t)$, and $u_1(t)$ is the square wave RF signal at the output of the RF signal generator RF1. The modulated light wave is transmitted through the optical fiber. At the receiver, PM2 modulates the incoming optical signal a second time by a phase shifted square wave, denoted by $u_2(t)$, which is output from RF2. Assuming no losses, the electric field at the

IEEE Transactions on Quantum Engineering

output of PM2 is given by

$$E_2(t) = \left\{ E_{\text{in}}(t) e^{\frac{j\pi u_1(t)}{V_\pi}} \right\} e^{\frac{j\pi u_2(t)}{V_\pi}}. \tag{2}$$

The RF waveforms, input to the phase modulators, can be expressed as $u_1(t) = p(\Omega t)$ and $u_2(t) = p(\Omega t - \phi)$ where

$$p(\Omega t) = \begin{cases} \frac{1}{2}, & \text{if } 0 < \Omega t \leq \pi \\ -\frac{1}{2}, & \text{if } \pi < \Omega t \leq 2\pi \\ p(\Omega t - 2\pi), & \text{otherwise} \end{cases} \tag{3}$$

and $\Omega = 2\pi/T$ is the repetition rate of the square wave signal $p(\Omega t)$, and ϕ is the phase difference between Alice and Bob's RF signals. With this, $E_2(t)$ becomes

$$E_2(t) = E_0 \exp\left[j\omega_0 t + jm\left\{ p(\Omega t) + p(\Omega t - \phi) \right\} \right] \tag{4}$$

where $m = \pi/V_\pi$. For simplicity, we assume same V_π for both PM1 and PM2. We also assume synchronized generation of the RF signals $u_1(t)$ and $u_2(t)$, which is accomplished by using same clock on both RF1 and RF2. Note that this limitation can be overcome by synchronizing the clocks through external means or on additional wavelength division multiplexing channel on the same fiber [14]. The waveform $p(\Omega t)$ can be expanded using Fourier series as

$$p(\Omega t) = \frac{2}{\pi} \sum_{l=1,3\ldots} \frac{1}{l} \sin(l\Omega t). \tag{5}$$

Then, $E_2(t)$ becomes

$$E_2(t) = E_0 e^{j\left[\omega_0 t + \sum_{l=1,3\ldots} \frac{4m}{l\pi} \cos\frac{l\phi}{2} \sin\left(l\Omega t - \frac{l\phi}{2}\right) \right]}. \tag{6}$$

To obtain the output power of the sidebands from (6), we use the Jacobi–Anger expression

$$e^{jz\sin\theta} = \sum_{n=-\infty}^{\infty} J_n(z) e^{jn\theta} \tag{7}$$

from which we obtain

$$E_2(t) = E_0 e^{j\omega_0 t} \prod_{l=1,3,5,\ldots,} \sum_{n=-\infty}^{\infty} J_n\left(\frac{4m}{l\pi} \cos\frac{l\phi}{2} \right) e^{j(ln\Omega t - ln\phi/2)}. \tag{8}$$

As seen from (8), the action of the two phase modulators results in the interference of the sidebands to generate a $\cos(l\phi/2)$ variation of the sideband at $\omega_l = \omega_0 + l\Omega$. Equation (8) can be simplified for the amplitudes of the carrier and the first sideband to obtain

$$E_2(t) = E_0 e^{j\omega_0 t} X(\phi) + E_0 e^{j[(\omega_0+\Omega)t - \phi/2)]} Y(\phi) \tag{9}$$

where $X(\phi)$ and $Y(\phi)$ are given by

$$\begin{aligned} X(\phi) &= J_0(z_1) J_0(z_3) J_0(z_5) \\ Y(\phi) &= J_1(z_1) J_0(z_3) J_0(z_5) + J_{-1}(z_1) J_{-1}(z_3) J_1(z_5) \end{aligned} \tag{10}$$

where the arguments of the Bessel functions z_l are given by

$$z_l(\phi) = \frac{4m}{l\pi} \cos\frac{l\phi}{2} \qquad \text{for } l = 1, 3, 5. \tag{11}$$

Contributions from the higher order Bessel functions $J_n(z)$ for $n \geq 2$ are negligible under the condition of low modulation index m. Also, higher harmonics of the RF signal $l \geq 7$ are ignored. Squaring $E_0 Y(\phi)$, and varying ϕ from 0 to 2π, we obtain the plot of the first sideband power versus ϕ, as shown in Fig. 2(a). Similarly, squaring $E_0 X(\phi)$, we obtain the plot of the carrier power versus ϕ, as shown in Fig. 2(b).

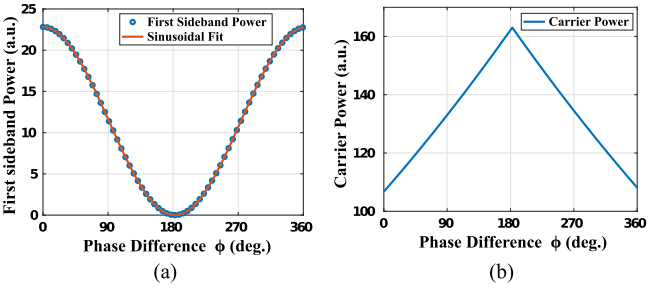


FIGURE 2. Plot of power of first sidebands $\omega_0 \pm \Omega$, and carrier ω_0 as function of phase difference ϕ between the RF signals generated by Alice and Bob.

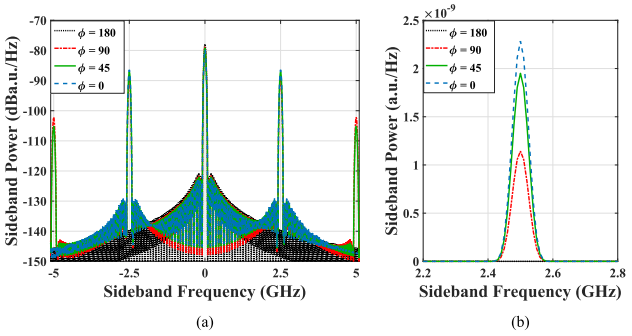


FIGURE 3. (a) Plot of PSD at the output of PM2 showing sideband interference. (b) Zoomed PSD of first sideband for phase differences of 0°, 45°, and 90°. Note that *y*-scale of (a) is in decibels, and *y*-scale of (b) is linear.

Fig. 3 shows the power spectral density (PSD) of $E_2(t)$ calculated using Welch technique for phase difference of 0°, 45°, 90°, and 180°. The optical filter is tuned to pass the first sideband $\omega_0 + \Omega$. We see that for a phase difference of 0°, sideband power is maximum, which corresponds to constructive interference. When the phase difference is 180°, the sideband power is minimum corresponding to destructive interference of the sideband. Thus, we find that by using a square RF waveform for modulation at Alice and Bob's ends, the setup shown in Fig. 1 generates sideband interference in the frequency domain. This principle can be used to synchronize the transmitter and receiver's clocks.

B. PROPOSED SYNCHRONIZATION PROCEDURE

We design a workflow that accomplishes the following two objectives of synchronization.

1) *Fine Synchronization:* The RF carriers need to be phase matched between points A and B, as shown in Fig. 1, for constructive and destructive interferences to occur. This ensures maximum interference visibility.
2) *Coarse Synchronization:* It is also necessary to ensure that during quantum transmission, Bob has the knowledge of the reference origin of Alice's clock.

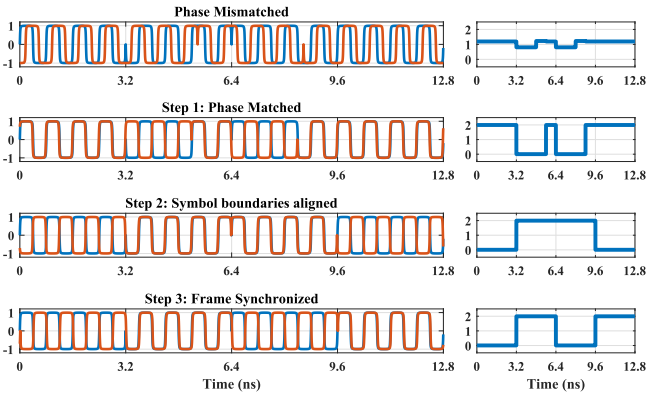


FIGURE 4. Steps in the proposed synchronization procedure. Optical phase at point A (blue) and electrical input to PM2 at point B (red). Waveforms in the right-hand side show the expected output from the photodetector at each step of the workflow.

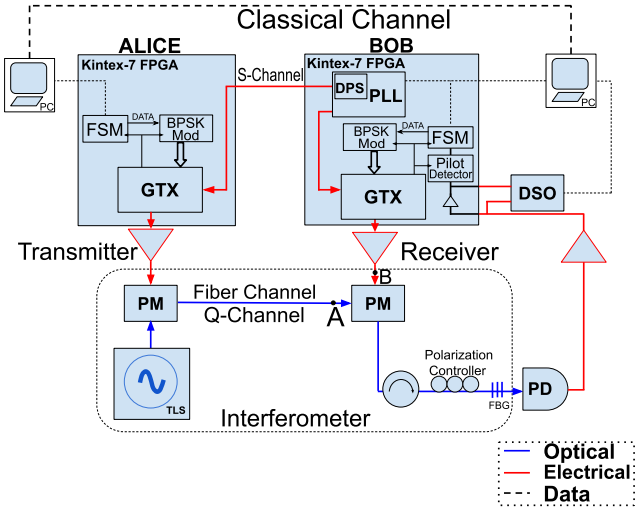


FIGURE 5. Experimental setup. Tunable laser source (TLS), phase modulator (PM), fiber Bragg grating (FBG), photodiode (PD), phase-locked loop (PLL), gigabit transceiver (GTX), dynamic phase shifter (DPS), finite-state machine (FSM), and digital storage oscilloscope (DSO).

This ensures that Bob can properly correlate his detections with the basis information Alice shares during the sifting phase of the QKD protocol.

The first objective requires a timing resolution much less than the RF carrier period ($\ll 400$ ps for 2.5 GHz). As shown in Fig. 2(a), the amplitude at the output of the interferometer is maximum when the RF phase difference is 0. Thus, we can monitor the interference amplitude by a photodetector, and maximize it by varying the phase delay of the RF carrier at Bob's end in the minimum possible step resolution of the RF source, i.e., 12.6 ps (FPGA's resolution). A resolution of a phase angle δ can reduce the maximum interference amplitude by an amount $\cos^2 \delta/4$ and similarly can increase the minimum interference amplitude by $\sin^2 \delta/4$, thus deteriorating the visibility to $\cos^2 \delta/4 - \sin^2 \delta/4 = \cos \delta/2$. Visibility loss due to the 12.6 ps resolution $= 1 - \cos(\pi 12.6/400) = 0.49\%$, which is small and neglected, considering the advantages of ease of implementation and robustness of the proposed scheme.

The second objective requires Alice and Bob to calibrate their respective clocks by performing interference using a known periodic data sequence. The sequence must be longer than the time that the optical signal takes to propagate through the fiber channel. In order to do this, Alice and Bob modulate their respective RF waveforms using BPSK modulation with a 256-b periodic sequence. The alternate bits of Bob's 256-b sequence are complemented, so that at the end of the synchronization procedure, the photodetector detects a signature of alternating constructive and destructive interference.

The workflow of the synchronization procedure, as illustrated in Fig. 4, is executed in the following three stages.

1) *Phase matching:* Maximize the interference amplitude by varying the phase delay of Bob's RF signal in steps of minimum resolution (12.6 ps for Kintex-7 FPGAs).
2) *Symbol boundary alignment:* Shift Bob's RF signal in increments of RF carrier period (400 ps for 2.5 GHz) till we observe zero pulses of width less than modulation symbol period in the interference detected. Any pulse of width less than the modulation symbol period indicate that the symbol boundaries are misaligned.
3) *Frame synchronization:* Shift Bob's RF signal in the steps of one symbol period (3.2 ns for 312.5 Msps modulation rate shown in Fig. 4) till a synchronization signature consisting of alternating constructive and destructive interference (156.25 MHz square waveform) is obtained. This ensures that Bob's clock is now synchronized with the reference origin Alice's clock, and the first symbol of Alice interferes with first symbol of Bob's and so on.

Note that this method performs synchronization from the "bottom–up" approach unlike typical methods, which perform "top–down" synchronization starting with frame synchronization. A successful detection of the signature pattern indicates that Alice and Bob are time synchronized with respect to each other.

III. EXPERIMENTAL SETUP

The technique of sideband interference for clock synchronization with square RF waveforms is implemented using FPGAs. Fig. 5 shows the experimental setup to observe the interference of sidebands in the frequency domain. Due to the stringent synchronization requirement to observe frequency-domain interference, the RF square waveforms at the transmitter and receiver are needed to be derived from a single seed clock. We use the clock at the receiver as the reference to derive the clocks needed by Bob's RF source, and also transmit another derived clock to the transmitter end by a separate synchronization (S) channel for Alice's RF source.

We used Kintex-7 series KC705 FPGA boards to generate electrical signals for the quantum (Q) channel and S-channel.

IEEE Transactions on Quantum Engineering

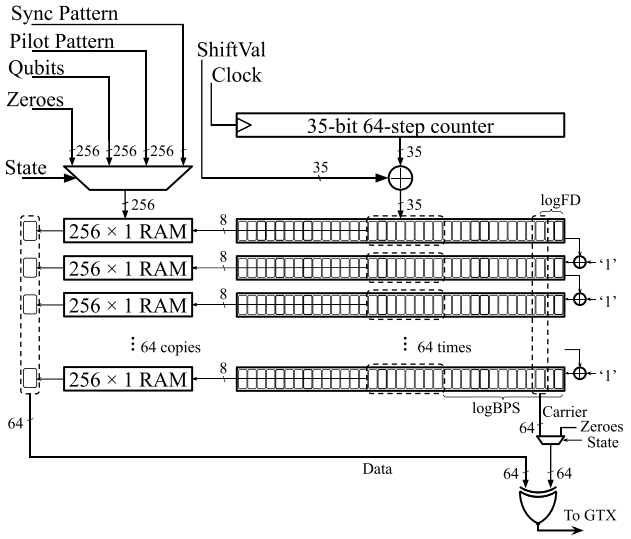


FIGURE 6. Waveform generator module implemented on Xilinx Kintex-7 FPGA for generating square RF BPSK modulation.

The KC705 FPGA board contains a GTX transceiver to generate a high-frequency RF signal for Q-channel. The GTX transceiver takes a 64-b parallel bus as input and serializes them into NRZ pulses at a maximum data rate of 10 Gsps (i.e., 5 GHz). The clock to the GTX transceiver is provided by the PLL implemented on the XC7K325T FPGA and the onboard Si570 oscillator programmed to generate the 156.25 MHz square wave clock. The PLL also generates a phase-shifted clock, whose phase can be dynamically configured using dynamic phase shifter, which is transmitted through the S-channel [37].

The signal from the GTX transceiver is amplified to obtain a 4 V_{pp}, which generates optical phase modulation at $\pi V/V_\pi = 0.8$ modulation depth. The optical carrier is obtained from a tunable laser source (Keysight N7714A) at a wavelength of 1550 nm and is phase modulated by an optical phase modulator (Thorlabs LN53S), with the modulation signal supplied from amplified GTX transceiver output. The phase-shifted clock signal from the receiver FPGA is sent to the transmitter FPGA on an RF cable, which acts as the S-channel. Alice uses the clock transmitted by Bob on the S-channel to clock her KC705 FPGA board's GTX transceiver. Note that for long distances, the phase shifted clock can be transmitted over a fiber link by intensity modulation at Bob's end and direct detection at Alice's end. The jitter introduced while transmitting the clock is cleaned by the internal MMCM/PLL block of the FPGA. An external jitter cleaner can be employed for better performance. The fiber link also causes phase drift, which can be compensated by the periodic execution of the synchronization procedure.

A. MODULATED WAVEFORM GENERATOR DESIGN

Fig. 6 shows the architecture of the modulated waveform generator module implemented on the FPGA. The output of this module is a 64-b parallel bus that, when input to the GTX transceiver, generates a BPSK modulated signal. The module allows for dynamic reconfiguration of carrier frequency and the modulation rate. In addition, for coarse-scale synchronization, the module allows provision for shifting the waveform in steps of 100 ps is provided. Postsynchronization, the same module can be used to generate the RF signal for qubit generation and measurement basis preparation during the quantum communication phase.

The functioning of the module is briefly summarized below.

1) The clock, recovered from the jitter cleaner module of the GTX transceiver, drives a 35-b counter. The frequency of the recovered clock is 10 Gsps/64 = 156.25 MHz.
2) The counter value increases at every clock edge in steps of 64. The user input `ShiftVal` is added to the current counter value. This addition results in a shift of the waveform by `ShiftVal`×100 ps. The added value is then incremented 63 times, creating an array of 64 35-b values.
3) Observe that if Nth bits of these 35-b values are collected, we obtain a carrier of frequency 5 GHz/2^N, where $N = 0, 1, \ldots, 34$ starts from 0. For example, if it is designed to generate an RF signal with a carrier frequency of 2.5 GHz, the frequency divider (FD) value is set to 5 GHz/2.5 GHz = 2, and $\log_2 2 = 1$. Thus, we set the value of logFD to 1 and collect the second LSBs of the 35-b values to obtain the square waveform RF carrier, as shown in Fig. 6.
4) To obtain the modulation data at the required data rate R, we calculate the required bits per symbol (BPS) = 10 Gsps/R. For example, for a data rate of 2.441 Msps, 10 Gsps/2.441 Msps = 4096, and $\log_2$ 4096 = 12. Thus, we set the value of logBPS = 12.
5) We use a 256-b data pattern for synchronization. For a data rate of 2.441 Msps, it takes $\tau_c = 256/2.441 = 104.8$ μs to transmit the pattern, which is sufficient to characterize the fiber channel length of up to $l = v\tau_c = 2 \times 10^8$ m/s × 104.8 μs = 21 km.
6) The 256-b data pattern is duplicated into 64 copies and stored in 64, 256 × 1 RAMs. These RAMs require $\log_2 256 = 8$-b address bus as input, which is fetched from the corresponding 35-b value. The position of the 8-b address starts from logBPS = 12th bit to 19th bit, as shown in Fig. 6.
7) The output of the 64 RAMs is collected and XORed with the carrier to generate the 64-b parallel bus of the modulated waveform, which can be input to the GTX transceiver.
8) The 256-b pattern to be modulated is decided by the state of the FSM. The 35-b counter loopbacks to 0 after $2^{35} \times 100$ ps= 3.2 s.

The spectrum of the BPSK modulated signal generated by the waveform generator module shown in Fig. 6 was measured using an RF spectrum analyzer (Agilent N9320).

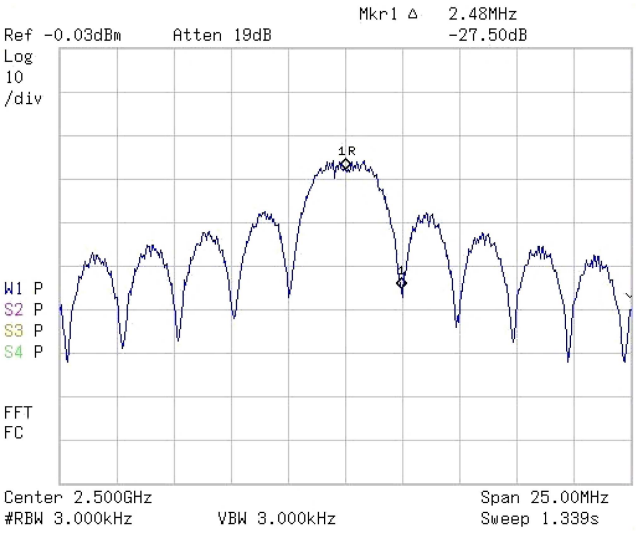


FIGURE 7. Measured spectrum of RF BPSK modulated signal generated by waveform generator module shown in Fig. 6. A 2^9-length PRBS was used as modulation data.

The measured RF spectrum is shown in Fig. 7. A 2^9-PRBS sequence was used as modulation signal in BPSK generation. The resolution bandwidth and video bandwidth of the spectrum analyzer was set to 3 kHz each. The result validates our approach of generation of BPSK signal using the scheme of Fig. 6.

B. FINITE-STATE MACHINE FOR QUANTUM COMMUNICATION

Upon performing the coarse and fine synchronization, the system implements qubit communication, where Alice transmits intended qubits and Bob performs interference on Alice's qubits synchronously. Alice cannot switch from sync sequence to quantum bits immediately after synchronization as Bob will be unable to decide the time instant at which the quantum interference should be initiated. We use an FSM implemented on the FPGA to address this problem as shown in Fig. 8.

Bob transmits a `syncAchieved` signal over the classical channel at the completion of coarse and fine synchronization, which arms Alice state machine for pilot transmission. Alice state machine waits for the 35-b counter to reset to 0 and then transmits the pilot sequence and initiates a timer through a 35-b counter. Alice again waits for the 35-b counter to loop back to 0 after pilot transmission by going to a crossover state `XOVR`. The `XOVR` state lasts 3.2 s, after which the quantum transmission begins. On Bob's side, the pilot detector module, as shown in Fig. 9, signals the state machine whenever the pilot signature is detected at the interferometer output. Upon detection of pilot, Bob's state machine goes to a `XOVR` state for 3.2 s, after which Bob starts to perform basis preparation for quantum communication. Placing a `XOVR` state has the following two reasons.

1) There is a delay between the interference of the pilot sequence and pilot signature detection by Bob's FPGA. Quantum communication should not start before the pilot signature detection because then Bob would not be ready with the basis preparation. That is why Alice has to begin quantum transmission only when her 35-b counter loops back to 0 after 3.2 s. Upon pilot signature detection, Bob waits for the 35-b counter to loop back to 0 and prepares basis when the counter is 0. With the `SYNC` state ensuring that Alice's and Bobs counter values are in sync, also ensures that Alice and Bob crossover state `XOVR` also ends synchronously.
2) Although the time delay between the pilot sequence interference and the pilot detection at Bob's FPGA is on a microsecond scale, the `XOVR` state is made to last for 3.2 s. This time is chosen in order for the classical laser source to be attenuated to ensure average photon per pulse is less than one and the classical photodetector to switch to operation in single-photon regime.

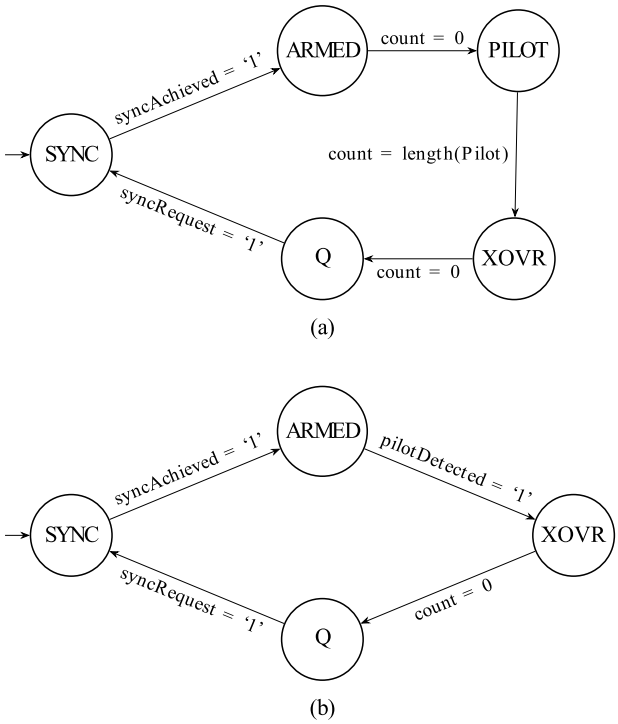


FIGURE 8. State diagram representation of the FSM modules implemented on the FPGAs at (a) Alice and (b) Bob.

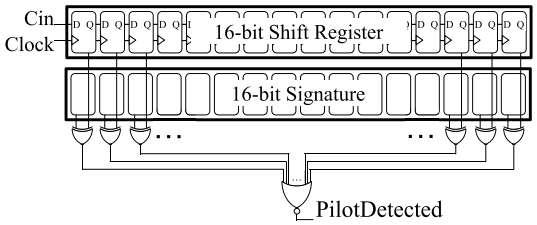


FIGURE 9. Pilot detector module implemented on Bob's FPGA.

After the crossover to `Q` state, Alice transmits qubits, and Bob prepares basis for measurement. After each frame of quantum communication (frame length decided a priori

IEEE Transactions on Quantum Engineering

TABLE 1. Resource Utilization Report of System Modules Implemented on Kintex-7 FPGA

Modules	Logic LUTs	Registers	MMCM	GTX
Top Module	11390 (5.59%)	5902 (1.45%)	3(30%)	1(25%)
Clocking	0	0	1	0
Modulator	7189 (3.53%)	38 (<0.01%)	0(0%)	0(0%)
GTX Transceiver	201 (0.1%)	305 (0.07%)	2 (20%)	1 (25%)
Pilot Detector	6 (<0.01%)	32 (<0.01%)	0(0%)	0 (0%)
VIO	266 (0.13%)	1331 (0.33%)	0 (0%)	0 (0%)
ILA	2909 (1.43%)	3652 (0.9%)	0 (0%)	0 (0%)

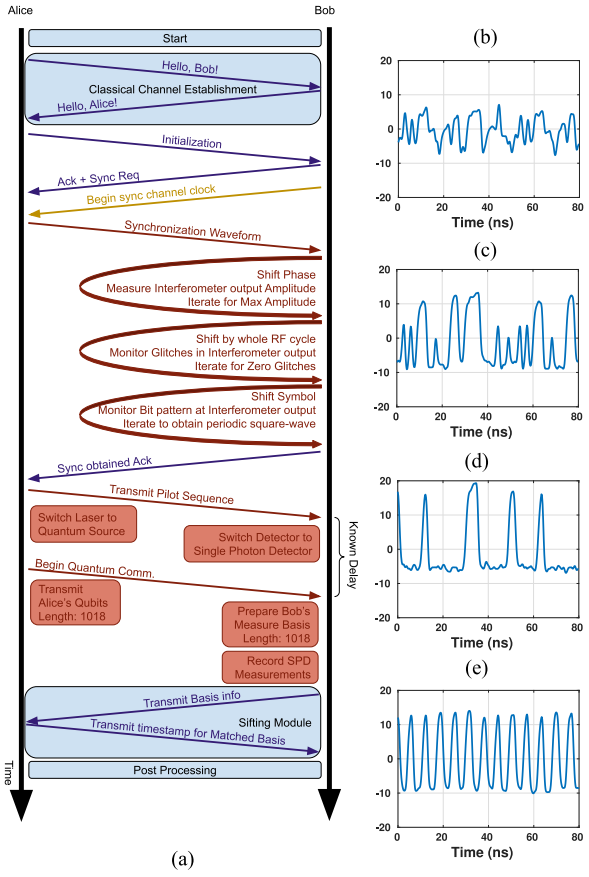


FIGURE 10. Workflow stack of Software defined FC-QKD. On the left-hand side is (a) lattice diagram showing the signaling between Alice and Bob on the three channels—blue: Classical channel (Ethernet), yellow: S-channel, and red: Q-channel. On the right-hand side are the DSO outputs at various stages of the synchronization. (a) Before synchronization, (b) phase matched, (c) symbol boundaries aligned, and (d) frame synchronized.

during classical channel establishment), sifting and postprocessing are performed. If needed, Bob carries out the synchronization procedure a second time for enhanced stability. The second synchronization also provides reset of the transmission.

Table 1 provides an overview of the device utilization, relative to the entire FPGA, for the various system modules reported in this.

IV. SYNCHRONIZATION WORKFLOW

We develop a workflow stack to operate the hardware system described in Section III. Fig. 10 shows the complete workflow stack for initialization, synchronization, quantum communication, and postprocessing steps for QKD. Alice and Bob handshake over an Ethernet channel using the representational state transfer application programming interface. Upon successfully validating the Ethernet connection, Bob transmits an initialization file in JSON format to Alice. This initialization file contains the values of the RF frequency, QKD protocol (BB84/B92), and the length of qubits in each frame.

Alice applies these parameters to the local FPGA module and transmits an acknowledgment signal. She then requests for the phase synchronization stage to begin. During the synchronization stage, Bob transmits the clock of frequency mentioned in the initialization file (156.25 MHz default) on the S-channel. This clock is derived using the reference seed oscillator on Bob's FPGA. Bob configures the phase of this clock, which will be configured dynamically for phase matching, as explained in Section IV-A. Bob also generates a clock derived from the same reference oscillator for clocking his own GTX transceiver. After receiving the signal from Bob on the S-channel, Alice clocks the GTX transceiver. She then transmits a periodic 256-b synchronization pattern ($0 \times$ B38E...) at a rate of 312.5 Mbps and an RF carrier at 2.5 GHz. Alice modulates this RF signal on the optical carrier using the optical phase modulator. Bob generates a similar 2.5 GHz RF signal with a data rate of 312.5 Msps, with the bits that are same as Alice's but with alternate bits complemented (i.e., $0 \times$ E6DB...). This is done so that upon synchronization, we obtain a clean square wave at the interferometer output, which is displayed and monitored on the DSO.

A. PHASE MATCHING

In the next step, Bob begins shifting the phase of the clock transmitted to Alice on the S-channel. Phase shifting of the clock is performed through the use of the FPGA's dynamic phase shifting module, which provides a minimum step delay of 12.6 ps for Kintex-7 FPGA. Bob increments the phase at this minimum resolution using a TCL script running in Vivado's virtual input/output module installed on a personal computer (PC). As shown in the simulation model of Fig. 1, as the RF phase difference between Alice and Bob decreases, the interferometer output is maximized. Bob monitors the interferometer output using a DSO, interfaced to the PC using MATLAB's instrument control toolbox.

Fig. 11 shows the peak-to-peak voltage measured at the interferometer output for varying phase differences between points A and B for Fig. 5. After detecting the interference maxima, Bob stops incrementing phase, and holding the last value of phase, Bob starts the next step of aligning the symbol boundaries. After phase synchronization, due to symbol boundary misalignment, pulses of widths less than the symbol period (3.2 ns for 312.5 Msps) will be seen on the interferometer output. The PC sends a command input to the FPGA to increment the `ShiftVal` register, thus shifting the RF waveform in the steps of 100 ps.

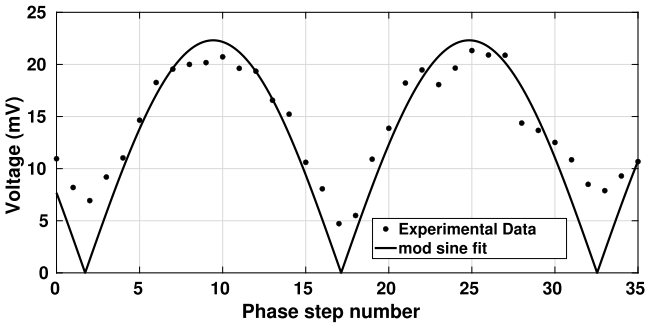


FIGURE 11. Peak-to-peak voltage monitored at the interferometer output versus RF phase difference between points A and B of experimental setup.

B. COARSE SYNCHRONIZATION

As the RF phases are synchronized, it is only necessary to shift Bob's waveform in increments of a whole RF cycle, which is 400 ps for a 2.5 GHz carrier, by assigning `ShiftVal` = 4 to align symbol boundaries. The PC iterates the shifts till it observes zero pulses of width less than the modulation symbol period. As the symbol boundaries are now aligned, the PC needs to shift Bob's waveform in increments of 1 symbol period, i.e., 3.2 ns. That is achieved by assigning `ShiftVal` = 32. The computer iterates this shifting till it observes a clean 156.25 MHz square wave on the interferometer output. A clean square wave output indicates that synchronization is achieved. Bob transmits a `syncAchieved` acknowledgment to Alice via a classical Ethernet channel.

C. TRANSITION TO QUANTUM COMMUNICATION

Upon receiving the `syncAchieved` acknowledgment from Bob, FSM module at Alice's FPGA proceeds to the `PILOT` state and the pilot pattern is transmitted to Bob. The pilot detector module at Bob's FPGA detects the pilot and the FSM at Bob's FPGA proceeds to the `XOVR` state of 3.2 s. During this state, Alice can attenuate the laser source using a variable optical attenuator such that the average photon per pulse in the sideband is less than one. Concurrently, Bob can switch the photodetector's bias from linear to Geiger-mode to operate in the single-photon regime. The processes of laser attenuation and photodetector switching can be completed in milliseconds. The FSM module is conservatively designed for a 3.2 s `XOVR` state, which can be reconfigured for a shorter duration if necessary. After the `XOVR` state, Alice encodes the random bits onto the phase of the RF carrier using the modulator waveform generator circuit, as shown in Fig. 6, and then modulates optical carrier with the RF signal to generate sidebands, which is transmitted. At the receiver, Bob further modulates the received photons with the RF waveform whose phase is encoded with random bits independently generated at the receiver. The sideband generated at the receiver interferes with that generated at the transmitter. If the bits encoded by Alice and Bob are equal, constructive interference takes place, and the probability of the photon detection at the output of the interferometer is high. While if the bits encoded by Alice and Bob are different, destructive interference takes place, and the probability of photon detection is low.

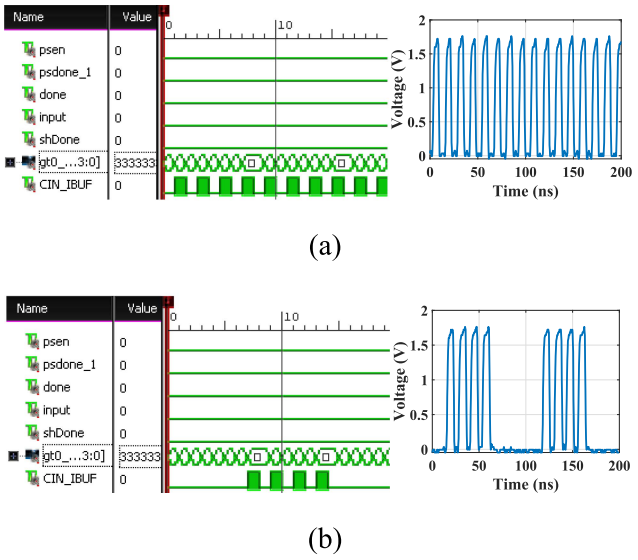


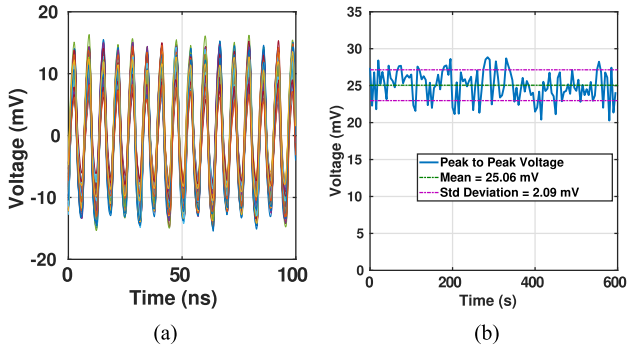
FIGURE 12. (a) Synchronization signature and (b) quantum transmission interference detected on Bob's FPGA and DSO (inset) when a qubit sequence of 0×8461... and 0×2E9E... was sent by Alice and Bob, respectively.

For validating that the proposed synchronization mechanism works, i.e., the first qubit of Alice interferes with the first qubit of Bob and so on, we assigned the Qubit register at Alice to be 0 × 8461... and the Qubit register at Bob to be 0 × 2E9E... and executed the synchronization workflow. The interferometer output was fed back to the FPGA at Bob's end for pilot detection and state transition purposes, and also buffered out through a general purpose output port of the FPGA for monitoring using DSO, as shown in Fig. 5.

Fig. 12(a) shows the synchronization signature detected by the FPGA and displayed using Vivado's integrated logic analyzer (ILA). Alternating logic high and low indicate that the three-stage synchronization is accomplished, after which Bob sent a `syncAchieved` acknowledgment to Alice. Fig. 12(b) shows the interference pattern caused by the Alice and Bob's qubit sequence 0 × 8461 and 0 × 2E9E. Note that the first 16 bits expected from the interference of the qubit sequences are 0 × 5500, which is observed on the Vivado ILA and also on the DSO. A logic high output from the FPGA indicates a high probability of photon detection by the SPD, whereas a logic low indicates a low probability of photon detection.

V. DISCUSSIONS

Our technique is based on frequency-domain interference and as such has a limitation that it is susceptible to thermal, mechanical, and environmental factors. In addition, the interference visibility is affected by the slow drift of optical components operating point and fiber-induced fluctuations during transmission, and detuning of the central wavelength of Bragg-grating-based optical filter. This can be overcome



(a) (b)

FIGURE 13. Plots to demonstrate interferometer stability. (a) Output of DSO synchronization signature monitored every 5 s for 10 min. (b) Peak-to-peak voltage of the synchronization signature with respect to time.

by the thermal isolation of the optical filter in an oven with a feedback temperature control. Interference is also affected by the group delay variations and polarization fluctuations in the optical fiber channel. The group delay fluctuations result in phase variation, which shifts the interferometer away from the phase-matched operating condition. Periodic execution of the synchronization procedure can be performed to stabilize the interferometer.

We measured the stability of our frequency-domain interferometer setup over a duration of 10 min, postsynchronization. We recorded the square waveform synchronization signature every 5 s. Fig. 13(b) shows the plot of the peak-to-peak voltage of the square waveform obtained at the output of the interferometer photodiode. The standard deviation and the mean peak-to-peak voltage were measured to be 2.1 and 25.06 mV, respectively.

In this work, we demonstrate synchronization using a frequency-domain interferometer, which is inherently supported for frequency-coded QKD. However, our technique of synchronization can be used to synchronize other implementations of QKD as well. In such scenarios, a frequency-domain interferometer needs to be implemented on a separate wavelength multiplexed over the same fiber as the quantum channel. This allows the interferometer to detect timing drifts due to the fiber channel, which can then be compensated for in the QKD system. Synchronization precision achieved would be higher because the frequency-domain interferometer is more sensitive to temporal fluctuations compared to existing synchronization methods.

We compare the precision of our synchronization technique with recent synchronization schemes. While direct comparison with existing literature is difficult due to significant differences in experimental setup and QKD protocol used, we have constructed a comparative table (see Table 2) to provide a contextual understanding of precision achieved in these studies relative to ours.

TABLE 2. Comparison of Synchronization Precision With Recent Methods

Reference	QKD Protocol	Precision
[38]	BB84	208 ps
[21]	Time-bin coded BBM92	250 ps
[39]	Time-bin coded BB84	$\approx$ 1 ns
[40]	Polarization coded BB84	467 ps
[41]	Time-bin coded high dimensional	20 ps
[42]	Polarization coded three-state BB84	1 ns
Our work	Frequency-coded configurable	12.6 ps

VI. CONCLUSION

We proposed and experimentally demonstrated a novel synchronization method for QKD systems. The method consisted of maximizing the visibility of frequency-domain interference of optical sidebands about an optical carrier at the receiver node. The sidebands were generated by phase modulation of the optical carrier by an RF signal whose phase can be dynamically varied. The phase-variable RF signal was generated by the FPGA at the transmitter and the receiver using GTX transceivers. In order to facilitate this, we used square waveforms for RF signal instead of the conventional sinusoidal signals. We derived mathematical expressions for sideband power as a function of the phase difference between RF signals at transmitter and receiver. The phase was adjusted using dynamic phase shifter module, implemented by the FPGA. We proposed a complete workflow that allowed transmitter and receiver synchronization to within 12.6 ps directly over the quantum channel of QKD systems. Once synchronized, the same system can be switched over to quantum transmission by user-defined time delay. The workflow was implemented on a Xilinx Kintex-7 KC705 FPGA board. Unlike other methods, our proposed system offered runtime changes in bit-rate, number of bits to qubit mapping, and periodic synchronization on Q-channel based on demand. The circuit modules utilized 5.6% of the LUT resources and 1.5% of the FPGA registers. We studied the robustness of our technique by evaluating the stability of the interferometer over an operation of 10 min with standard deviation of interference to be less than 9% of the mean detection amplitude. In our future work, we are analyzing the long-term stability of our method through additional experiments. The mitigation techniques we are currently implementing include polarization stabilization of the link through automatic electronic polarization controller, isolation of critical optical components, and monitoring visibility for adaptively changing phase shifter from FPGA.

ACKNOWLEDGMENT

The authors sincerely thank the reviewers for all the valuable comments and suggestions, which helped in improving the quality of this article.

REFERENCES

[1] R. J. Aliaga, J. M. Monzó, M. Spaggiari, N. Ferrando, R. Gadea, and R. J. Colom, "PET system synchronization and timing resolution using high-speed data links," *IEEE Trans. Nucl. Sci.*, vol. 58, no. 4, pp. 1596–1605, Apr. 2011, doi: 10.1109/TNS.2011.2140130.

[2] Y. Hu, Y. Wang, J. Kuang, and B. Wu, "A clock distribution and synchronization scheme over optical links for large-scale physics experiments," *IEEE Trans. Nucl. Sci.*, vol. 68, no. 6, pp. 1351–1358, Jun. 2021, doi: 10.1109/TNS.2021.3070589.

[3] A. Mahmood, R. Exel, H. Trsek, and T. Sauter, "Clock synchronization over IEEE 802.11—A survey of methodologies and protocols," *IEEE Trans. Industr. Inform.*, vol. 13, no. 2, pp. 907–922, Apr. 2017, doi: 10.1109/TII.2016.2629669.

[4] A. Pljonkin and K. Rumyantsev, "Single-photon synchronization mode of quantum key distribution system," in *Proc. 2016 Int. Conf. Comput. Techn. Inf. Commun. Technol.*, New Delhi, India, 2016, pp. 531–534, doi: 10.1109/ICCTICT.2016.7514637.

[5] M. Bloch, S. W. McLaughlin, J. M. Merolla, and F. Patois, "Frequency-coded quantum key distribution," *Opt. Lett.*, vol. 32, no. 3, pp. 301–303, 2007, doi: 10.1364/OL.32.000301.

[6] P. Kumar and A. Prabhakar, "Bit error rates in a frequency coded quantum key distribution system," *Opt. Commun.*, vol. 282, no. 18, pp. 3827–3833, 2009, doi: 10.1016/j.optcom.2009.06.030.

[7] A. Pljonkin, K. Rumyantsev, and P. Kumar Singh, "Synchronization in quantum key distribution systems," *Cryptography*, vol. 1, no. 3, p. 18, 2017, doi: 10.3390/cryptography1030018.

[8] P. Liu and H. L. Yin, "Secure and efficient synchronization scheme for quantum key distribution," *OSA Continuum*, vol. 2, no. 10, pp. 2883–2890, 2019, doi: 10.1364/OSAC.2.002883.

[9] G. Vallone et al., "Adaptive real time selection for quantum key distribution in lossy and turbulent free-space channels," *Phys. Rev. A.*, vol. 91, no. 4, Apr. 2015, Art. no. 042320, doi: 10.1103/PhysRevA.91.042320.

[10] J. P. Bourgoin et al., "Experimental quantum key distribution with simulated ground-to-satellite photon losses and processing limitations," *Phys. Rev. A.*, vol. 92, no. 5, Nov. 2015, Art. no. 052339, doi: 10.1103/PhysRevA.92.052339.

[11] S. Lacheta, A. Agrawal, M. K. Jain, R. S. Urdhwareshe, S. Goyal, and P. K. Gupta, "Timing synchronization in an FPGA-based real-time quantum key distribution system," in *Proc. 2023 IEEE Microw., Antennas, Propag. Conf.*, 2023, pp. 1–4, doi: 10.1109/MAPCON58678.2023.10464161.

[12] N. Walenta et al., "A fast and versatile quantum key distribution system with hardware key distillation and wavelength multiplexing," *New J. Phys.*, vol. 16, no. 1, 2014, Art. no. 013047, doi: 10.1088/1367-2630/16/1/013047.

[13] B. Korzh et al., "Provably secure and practical quantum key distribution over 307 km of optical fibre," *Nat. Photon.*, vol. 9, no. 3, pp. 163–168, Mar. 2015, doi: 10.1038/nphoton.2014.327.

[14] O. L. Guerreau, J. M. Mérolla, A. Soujaeff, F. Patois, J. P. Goedgebuer, and F. J. Malassenet, "Long-distance QKD transmission using single-sideband detection scheme with WDM synchronization," *IEEE J. Sel. Top. Quantum Electron.*, vol. 9, no. 6, pp. 1533–1540, Nov./Dec. 2003, doi: 10.1109/JSTQE.2003.820929.

[15] T. F. da Silva and J. P. von der Weid, "Optical transmission of frequency-coded quantum bits with WDM synchronization," *J. Microw. Optoelectron. Electromagn. Appl.*, vol. 8, no. 1, pp. 163S–178S, Jun. 2009, doi: 10.14209/sbrt.2008.42879.

[16] R. Shakhovoy et al., "Wavelength-and time-division multiplexing via pump current variation of a pulsed semiconductor laser—A method of synchronization for quantum key distribution," *IEEE J. Quantum Electron.*, vol. 59, no. 1, Feb. 2023, Art. no. 8000110, doi: 10.1109/JQE.2023.3237265.

[17] R. D. Cochran and D. J. Gauthier, "Qubit-based clock synchronization for QKD systems using a Bayesian approach," *Entropy*, vol. 23, no. 8, Jul. 2021, Art. no. 988, doi: 10.3390/e23080988.

[18] L. Calderaro et al., "Fast and simple qubit-based synchronization for quantum key distribution," *Phys. Rev. Appl.*, vol. 13, no. 5, May 2020, Art. no. 054041, doi: 10.1103/PhysRevApplied.13.054041.

[19] Y. Chen, C. Huang, G. Lin, S. Huang, Z. Zhang, and K. Wei, "Qubit-based distributed frame synchronization for quantum key distribution," *J. Lightw. Technol.*, early access, Sep. 19, 2024, doi: 10.1109/JLT.2024.3464750.

[20] C. Huang et al., "A cost-efficient quantum access network with qubit-based synchronization," *Sci. China Phys. Mech. Astron.*, vol. 67, no. 4, Apr. 2024, Art. no. 240312, doi: 10.1007/s11433-023-2302-8.

[21] E. Fitzke et al., "Scalable network for simultaneous pairwise quantum key distribution via entanglement-based time-bin coding," *PRX Quantum*, vol. 3, no. 2, May 2022, Art. no. 020341, doi: 10.1103/PRXQuantum.3.020341.

[22] Y. Wang, J. Kuang, C. Liu, and Q. A. Cao, "A 3.9-ps RMS precision time-to-digital converter using ones-counter encoding scheme in a Kintex-7 FPGA," *IEEE Trans. Nucl. Sci.*, vol. 64, no. 10, pp. 2713–2718, Oct. 2017, doi: 10.1109/TNS.2017.2746626.

[23] H. B. Xie, Y. Li, Q. Shen, S. K. Liao, and C. Z. Peng, "A high-precision 2.5-ps RMS time synchronization for multiple high-speed transceivers in FPGA," *IEEE Trans. Nucl. Sci.*, vol. 66, no. 7, pp. 1070–1075, Jul. 2019, doi: 10.1109/TNS.2019.2904703.

[24] Q. Shen et al., "An FPGA-based TDC for free space quantum key distribution," *IEEE Trans. Nucl. Sci.*, vol. 60, no. 5, pp. 3570–3577, Oct. 2013, doi: 10.1109/TNS.2013.2280169.

[25] T. Sui et al., "2.3-ps RMS resolution time-to-digital converter implemented in a low-cost cyclone V FPGA," *IEEE Trans. Instrum. Meas.*, vol. 68, no. 10, pp. 3647–3660, Oct. 2019, doi: 10.1109/TIM.2018.2880940.

[26] M. Zhang, K. Yang, Z. Chai, H. Wang, Z. Ding, and W. Bao, "High-resolution time-to-digital converters implemented on 40-, 28-, and 20-nm FPGAs," *IEEE Trans. Instrum. Meas.*, vol. 70, 2021, Art. no. 2002310, doi: 10.1109/TIM.2020.3036066.

[27] M. Zhang, H. Wang, and Y. Liu, "7.4 ps FPGA-based TDC with a 1024-unit measurement matrix," *Sensors*, vol. 17, no. 4, Apr. 2017, Art. no. 865, doi: 10.3390/s17040865.

[28] J. Wu, "Several key issues on implementing delay line based TDCs using FPGAs," *IEEE Trans. Nucl. Sci.*, vol. 57, no. 3, pp. 1543–1548, Jun. 2010, doi: 10.1109/TNS.2010.2045901.

[29] A. Stanco et al., "Versatile and concurrent FPGA-based architecture for practical quantum communication systems," *IEEE Trans. Quantum Eng.*, vol. 3, Jan. 2022, Art. no. 6000108, doi: 10.1109/TQE.2022.3143997.

[30] N. Venkatachalam, F. P. Shingala, C. Selvagangai, S. Dillibabu, P. Chandravanshi, and R. P. Singh, "Scalable QKD post processing system with reconfigurable hardware accelerator," *IEEE Trans. Quantum Eng.*, vol. 4, 2023, Art. no. 4100914, doi: 10.1109/TQE.2023.3326093.

[31] B. Kebapci et al., "FPGA-based implementation of an underwater quantum key distribution system with BB84 protocol," *IEEE Photon. J.*, vol. 15, no. 4, Aug. 2023, Art. no. 7600210, doi: 10.1109/JPHOT.2023.3287493.

[32] J. Constantin et al., "An FPGA-based 4 Mbps secret key distillation engine for quantum key distribution systems," *J. Signal Process. Syst. Signal Image Video Technol.*, vol. 86, no. 1, pp. 1–15, Jan. 2017, doi: 10.1007/s11265-015-1086-1.

[33] O. L. Guerreau, F. J. Malassenet, S. W. McLaughlin, and J. M. Merolla, "Quantum key distribution without a single-photon source using a strong reference," *IEEE Photon. Technol. Lett.*, vol. 17, no. 8, pp. 1755–1757, Aug. 2005, doi: 10.1109/LPT.2005.851050.

[34] O. G. Morozov, A. J. Sakhabutdinov, G. A. Morozov, and M. G. Il'daris, "Universal microwave photonics approach to frequency-coded quantum key distribution," *Adv. Technol. Quantum Key Distrib.*, vol. 20, pp. 113–133, Dec. 2017, doi: 10.5772/intechopen.71974.

[35] P. Kumar, "Optical modulation schemes for frequency-coded quantum key distribution," in *Proc. IEEE 2010 Nat. Conf. Commun.*, Jan. 2010, pp. 1–5, doi: 10.1109/NCC.2010.5430155.

[36] A. V. Gleim et al., "Secure polarization-independent subcarrier quantum key distribution in optical fiber channel using BB84 protocol with a strong reference," *Opt. Exp.*, vol. 24, no. 3, pp. 2619–2633, Feb. 2016, doi: 10.1364/OE.24.002619.

[37] AMD, "7 Series FPGAs clocking resources," Adv. Micro Devices, Santa Clara, CA, USA, 2018, [Online]. Available: https://xilinx.com/support/documentation/user_guides/ug472_7Series_Clocking.pdf

[38] C. Wang et al., "Robust aperiodic synchronous scheme for satellite-to-ground quantum key distribution," *Appl. Opt.*, vol. 60, no. 16, pp. 4787–4792, Jun. 2021, doi: 10.1364/AO.425085.

[39] N. S. Aseri et al., "FPGA based quantum key distribution electronic system for multipurpose optical setup and protocols," in *Proc. J. Phys.: Conf. Ser.*, Feb. 2021, Art. no. 012047, doi: 10.1088/1742-6596/1755/1/012047.

[40] A. V. Miller, "A fast and efficient algorithm for time synchronization in satellite quantum key distribution," in *Proc. J. Phys.: Conf. Ser.*, Feb. 2024, Art. no. 012017, doi: 10.1088/1742-6596/2701/1/012017.

[41] J. Williams, M. Suchara, T. Zhong, H. Qiao, R. Kettimuthu, and R. Fukumori, "Implementation of quantum key distribution and quantum clock synchronization via time bin encoding," *Proc. SPIE*, vol. 11699, pp. 16–25, 2021, doi: 10.1117/12.2581862.

[42] F. Berra et al., "Synchronization of quantum communications over an optical classical communications channel," *Appl. Opt.*, vol. 62, no. 30, pp. 7994–7999, Oct. 2023, doi: 10.1364/AO.500416.