Time-Bin Superposition Methods for DPS-QKD

Gautam Shaw, *Member, IEEE*, Shyam Sridharan, Shashank Ranu, Foram Shingala, Prabha Mandayam, and Anil Prabhakar

***Abstract*—Key generation efficiency, and security, in differential phase-shift quantum key distribution (DPS-QKD) improve with an increase in the number of optical delays or time-bin superpositions. We demonstrate the implementation of superposition states using time-bins, with two different approaches. In Type-A, we use an optical pulse and create superposition states with optical splitters and path delays. Similar superposition states are created, in Type-B, by applying direct phase modulation within a single weak coherent pulse. We establish the equivalence between both the approaches, and note that higher-order superposition states of Type-B are easier to generate for DPS-QKD. We set up DPS-QKD, over 105 km of single mode optical fiber, with a quantum bit error rate of less than 15% at a secure key rate of 2 kbps. With temporal guard bands, the QBER reduced to less than 10%, but with a 20% reduction in the key rate.**

***Index Terms*—Differential phase, QBER, quantum key distribution, secure key, time-bin superposition methods.**

I. Introduction

QUANTUM key distribution (QKD) enables secure key exchange between authenticated users, Alice and Bob, by relying on two aspects of quantum mechanics, Heisenberg's uncertainty principle and the no-cloning theorem [1]. When an adversary, Eve, attempts to steal information from the quantum channel, she also inevitably introduces disturbances in the channel and reveals herself. Since the first proposal by Bennett and Brassard in 1984 [2], there have been a variety of QKD protocols, both proposed and implemented [3], [4], [5], [6]. Long distance field demonstrations of QKD mostly use discrete variables, some with active stabilization to mitigate environmental fluctuations [7]. In Appendix A, we provide the reader with a quick summary of key rates and channel lengths for a few recent implementations of QKD.

This article aims to establish the equivalence between two different time-bin superposition states for use in a differential phase-shift quantum key distribution (DPS-QKD) system. DPS-QKD as proposed by Inoue et al., is simple to implement and robust against slowly varying environmental fluctuations [6], [8]. DPS-QKD uses a pair of phases $\Phi = \{0, \pi\}$ to generate non-orthogonal states that cannot be distinguished with absolute certainty using a single measurement [9]. A theoretical security proof of the DPS protocol, with single photons and weak coherent sources, was established under the assumption that Eve is restricted to individual attacks and also it was concluded that individual attacks are more powerful than sequential attacks [10], [11]. An efficient phase encoding quantum key generation scheme, with narrow band heralded photons, was proposed by Yan et al., where key information is carried by the phase modulation directly on the single-photon temporal waveform [12], [13]. Time-bin qubits, composed of temporal modes with weak coherent sources, are effective constituents to build a robust and simple QKD system with a high secure key rate [14]. To increase the secure key rate, with minimum resources, researchers have used two-dimensional and four-dimensional QKD protocols with time-bin and phase encoding [15]. Dellantonio et al. proposed two equivalent high dimensional MDI-QKD methods: space and time-bin encoding, which uses space to encode information in different paths and time-slots to encode qudits [16]. In high dimensional QKD protocols, multiple bits of information are encoded on a single state, hence, it increases the channel capacity and is more robust against channel noise.

The recently introduced round-robin differential phase-shift quantum key distribution (RR-DPS-QKD) scheme addresses the effects of environmental disturbances, and gives us an upper bound on our tolerance to error rates with a bit error rate as high as 29% [17]. But such schemes requires the addition of optical switches and delays that make Bob's set-up more complex [18].

In Section IV, we describe two schemes, Type-A and Type-B, that yield comparable key rates in kbps, with a QBER < 0.2. Time-bins, in Type-B are defined electronically and are significantly easier to generate, making them more amenable to Si-photonics implementations. The scheme does require more precise timing synchronization, and we have developed the means to characterize the photon arrival time at our detector to within 50 ps. We further demonstrate that the use of one temporal multiplexed single photon detector along with temporal filtering can reduce the quantum bit error rate (QBER) of our DPS-QKD implementation, but at a reduced secure key rate.

II. Experimental Setup

In the first DPS-QKD proposal, a single photon was allowed to pass through a beam splitter, travel through different path delays and then recombined to create a superposition state of

Manuscript received 10 July 2022; revised 24 August 2022; accepted 2 September 2022. Date of publication 7 September 2022; date of current version 20 September 2022. This work was supported by the Ministry of Human Resource Development under Grant 35-8/2017-TS. *(Corresponding author: Gautam Shaw.)*

Gautam Shaw, Shyam Sridharan, Foram Shingala, and Anil Prabhakar are with the Department of Electrical Engineering, Indian Institute of Technology Madras, Chennai, TN 600036, India (e-mail: ee15d047@ee.iitm.ac.in; ee17s018@smail.iitm.ac.in; foram.shingala@gmail.com; anilpr@ee.iitm.ac.in).

Shashank Ranu is with the Department of Electrical Engineering, Indian Institute of Technology Madras, Chennai, TN 600036, India, and also with the Department of Physics, Indian Institute of Technology Madras, Chennai, TN 600036, India (e-mail: ee16s300@ee.iitm.ac.in).

Prabha Mandayam is with the Department of Physics, Indian Institute of Technology Madras, Chennai, TN 600036, India (e-mail: prabhamd@iitm.ac.in).

Digital Object Identifier 10.1109/JPHOT.2022.3204920

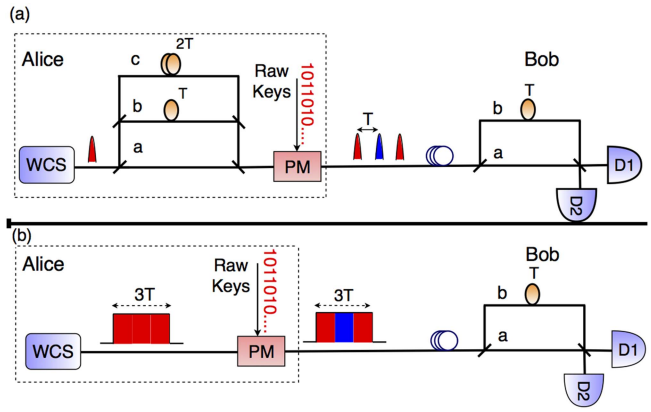

Fig. 1. 4-state DPS-QKD with a weak coherent source (WCS). Superposition states are generated as (a) Type-A : with optical splitters and delay lines, followed by a phase modulator (PM) and (b) Type-B : phase encoded pattern is applied directly within a weak coherent pulse. T: time, D1 and D2: single photon detectors.

the photon [6]. However, this scheme would encounter beam splitter losses and reduces the secure key rate. The more common version of DPS-QKD is one that uses weak coherent pulses (WCPs) [19]. A relative phase of $\{0, \pi\}$ is applied over adjacent time-bins, and hence the photon will be in a superposition of 2^{N-1} states.

We propose a similar, yet simpler method, wherein superposition states are generated by adding a relative phase at $N-1$ locations within a single weak coherent pulse. We demonstrate the equivalence of this method, called Type-B, over the conventional Type-A method that uses the phase difference between many optical pulses within the coherence time of a laser. In this article, we define 2^{N-1} as M, and hence, refer to the 3-pulse DPS-QKD as a 4-state system. This notation will allow us to describe the creation of superposition states by temporal phase modulation.

We describe our experiments with 4-state DPS-QKD, using two different time-bin superposition methods, as shown in Fig. 1. Time-bin superposition states, from Type-B, are easier to implement and control, and can be extended to an M-state DPS-QKD scheme without any additional hardware complexity. When we use a superposition of 4 states, an intercept and resend (IR) attack by Eve introduces a 33% error on the sifted key. We had previously reported that the 4-state DPS scheme is more secure against both IR and beam splitter attacks [20]. This percentage error increases to 50% when 4-state DPS is extended to M-state DPS, but with ideal detectors [20]. The methodology used to implement a weak coherent source (WCS) is described along with the rest of our experimental setup in Section IV-A.

III. Key Generation in DPS-QKD

In our 4-state DPS-QKD implementation. Alice sends a single photon in a superposition of 3 time-bins to Bob. The probability of a photon traveling through one of the 3 paths in Alice's set-up is $1/3$. The superposition state generated from Alice is

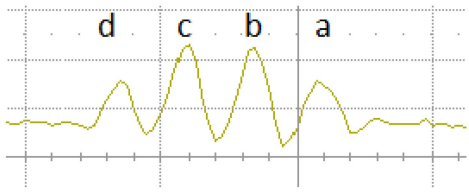

Fig. 2. Photodetector output after Alice's time-bin superposition and Bob's DLI, captured with a diode laser source. The key is generated by the interference in time-bins b and c.

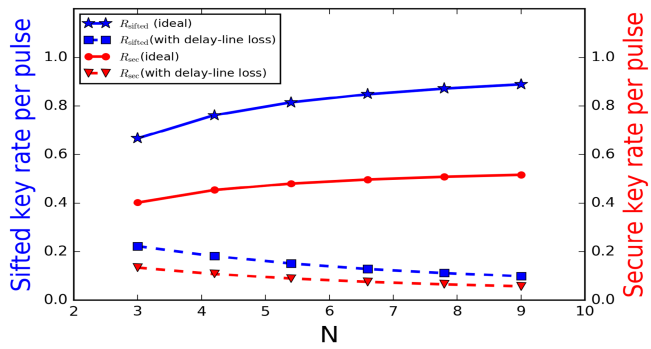

Fig. 3. Estimates for the sifted and secure key rate for M-state DPS-QKD, with ideal detectors, where $M = 2^{N-1}$.

represented as:

$$|\Psi\rangle = \frac{1}{\sqrt{3}}\left[|1\rangle_a|0\rangle_b|0\rangle_c \pm |0\rangle_a|1\rangle_b|0\rangle_c \pm |0\rangle_a|0\rangle_b|1\rangle_c\right] \quad (1)$$

$$\triangleq \frac{1}{\sqrt{3}}\left[|100\rangle_{abc} \pm |010\rangle_{abc} \pm |001\rangle_{abc}\right] \quad (2)$$

where the paths a, b, c also represent time-bins. $|\Psi\rangle$ is passed through a delay line interferometer (DLI) at Bob's site. As a result, the photon is now in a superposition of 4 time-bins. The first and last time-bins do not contain encoded phase difference information, whereas the 2 central time-bins contribute to the key generation. The 4 time-bins can also be observed classically, but at higher photon numbers, as shown in Fig. 2. Alice now encodes her random key bit as a random phase $\phi = \{0, \pi\}$ between successive time-bins. Bob extracts the key information using a DLI and two single-photon detectors. Eve's intercept and resend attack introduces an error of 33% in the sifted key in the 4-state DPS compared to the 25% error when using a train of WCPs in conventional DPS-QKD.

The secure key rate (R_{sec}) is estimated from sifted key rate (R_{sifted}) as

$$R_{\text{sec}} = R_{\text{sifted}}\left[\tau - f(e)h(e)\right], \quad (3)$$

where τ is the shrinking factor, $f(e)$ captures the inefficiency of the error correcting code, and $h(e)$ is the binary Shannon entropy. The error rate, e, depends upon dark counts and other system imperfections and τ captures Eve's knowledge of the key. If we assume Eve's attack to be limited to the IR and beamsplitter attacks, increasing N changes the efficacy of the attacks, thus making τ a function of N [20]. Hence, a secure key rate that depends on both R_{sifted} and τ, varies with N as shown in Fig. 3.

Experimentally, the generation of a superposition state can be realized using passive beam splitters (or beam combiners) and optical delay lines, Type-A in Fig. 1. However, passive beam splitters have insertion losses and the sifted key rate is reduced by a factor of N, thus making the implementation inefficient. An implementation with $N = 3$ yields $M = 4$ non-orthogonal states that Alice then uses to transmit a raw key. Keeping in mind the ease of implementing time-bin superposition, and also the move towards a Si-photonics platform, we advocate the Type-B approach of phase modulation. This would potentially allow us to use $N > 3$ and obtain a higher sifted key rate, as seen in Fig. 3. However, with non-ideal SPDs, the optimal value against all attacks is $N = 3$ [11]. We observe this by the increase in dark counts and afterpulsing, leading to a deterioration in secure key rate as N increases [21]. The power splitters in the Type-A scheme introduce an extra loss. Thus, for a weak coherent source with the same output mean photon number, we expect a reduction in transmitted raw key rate and a corresponding reduction in sifted and secure key rates, as shown in Fig. 3.

IV. Experimental Results

The state at the output port of Bob's DLI, consists of a single photon in one of 4 time-bins. A correct identification of these time-bins needs an accurate temporal characterization of the single photon detector (SPD), and its associated electronics.

A. Experimental Set-up

Alice's set-up consists of a continuous laser source at 1550.12 nm and a RF pulse generator. A train of electrical pulses, having a pulse width of 500 ps and a time period of 32 ns, is applied to a 10 GHz intensity modulator (IM). The bias voltage to the IM was optimized to get a modulation extinction ratio of more than 14 dB. The resultant optical pulses were then attenuated, using a variable optical attenuator (VOA), to a mean photon number $\mu \sim 0.1$, and the photons were sent directly to a gated SPD. We observed 31 K counts/s when the gate window was synchronized with the photon arrival time. This reduced to around 1 K counts/s when the gate was out of sync with the arrival time of the photons.

Two different source configurations, Type-A and Type-B shown in Fig. 4, were then used in the DPS-QKD experimental set-up shown in Fig. 5 . In Fig. 4(a), weak coherent pulses are passed through 1×3 and 3×1 beam splitter-coupler combination and optical delay lines so that photons coming out from 3×1 coupler are in superposition of three time-bins before being passed through the phase modulator (PM), shown in Fig. 5. In Fig. 4(b), a 3 ns pulse coming out of the intensity modulator (IM) is attenuated and acts as a weak coherent pulse. Phase modulation pattern can be applied directly on this WCP, as shown in Fig. 4(c).

One problem with using two independent detectors to differentiate between 0 and 1 bits is that the detectors are not identical, and will typically have different quantum efficiencies. We mitigate this by using time-multiplexing and capture photon arrival times from both output ports of the DLI. A fiber delay of

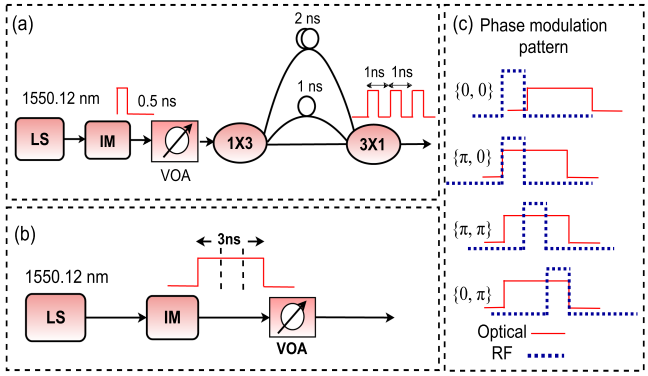

Fig. 4. Time-bin superposition states created with two methods (a) Type-A, and (b) Type-B. LS: laser source, IM: intensity modulator, VOA: variable optical attenuator. (c) Phase modulation pattern.

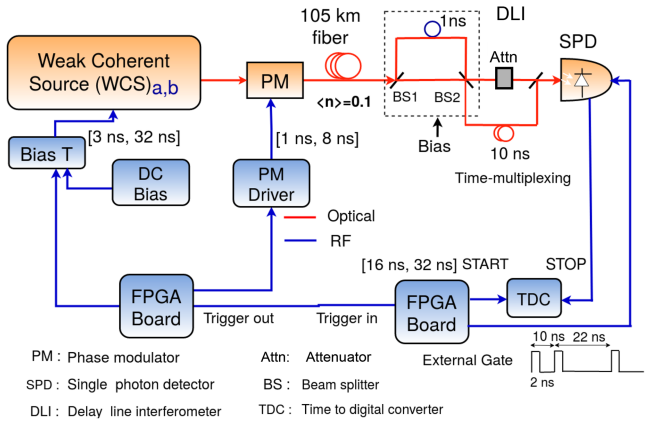

Fig. 5. 4-state DPS-QKD experimental set-up. Red and blue coloured blocks represent electro-optic and electrical (RF) devices used in the test-bed respectively. A detailed schematic of the weak coherent source is shown in Fig. 4.

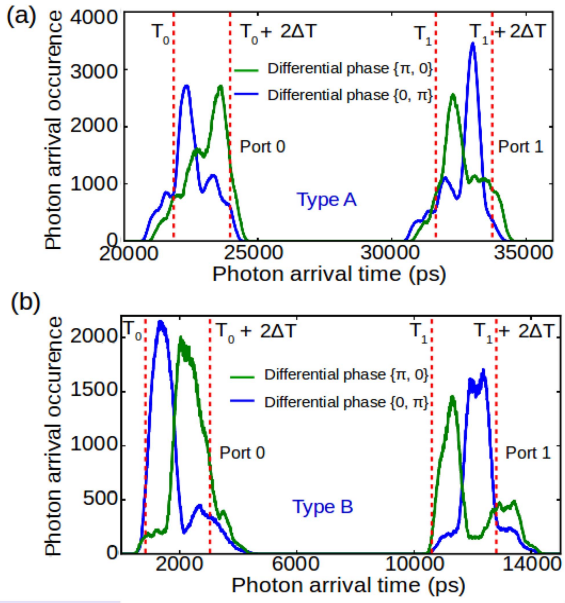

Fig. 6. Photon arrival time distribution for two time-bin superposition methods (a) Type-A and (b) Type-B.

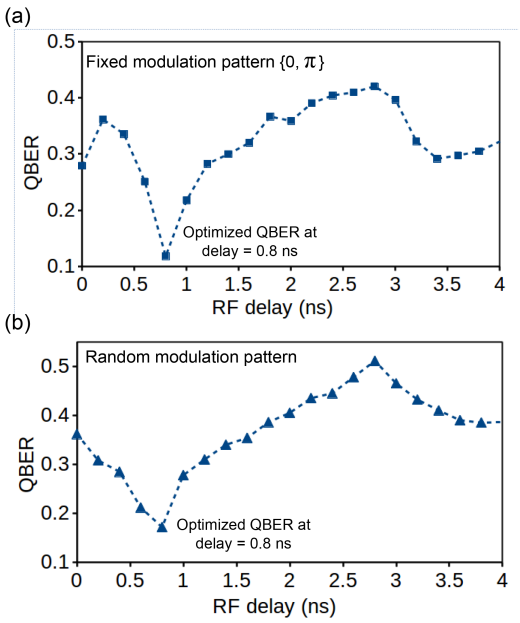

Fig. 7. Optimization of QBER by adjusting the timing of the applied phase (a) with fixed phase modulation pattern (b) with random phase modulation pattern.

10 ns was added at one of the output ports of the DLI. To equalize the loss in both paths from output ports of DLI, an attenuator of 0.5 dB was added in short path. Both ports were then multiplexed using a 2×1 coupler and sent to a SPD. This technique provides a cost-effective configuration since one SPD is enough to extract timing instant information. Unfortunately, half of the photons are lost due to the 2×1 combiner before the SPD. But, since we can generate WCPs at GHz rates, we are limited only by the hold-off time on the SPD and do not perceive any disadvantage to using a time-multiplexed configuration with a single SPD. Instead, using a single detector has the advantage of providing an equal sensitivity on both constructive and destructive interference ports of the DLI. An IM with a high extinction ratio reduces false detections during the 10 ns off time in the time-multiplexed detection scheme. The effect of dark count rate (DCR) in QBER for a time-multiplexed configuration is described along with the rest of source of errors in Section V-B.

A field programmable gate array (FPGA) is triggered synchronous to the pulse generator and it is configured to generate control signals for the SPD, TDC and a modulating signal (RF pulses) for the PM. Phase encoding patterns $\{0, 0\}$, $\{\pi, 0\}$, $\{0, \pi\}$ and $\{\pi, \pi\}$ are realized by applying RF pulses to the phase modulator synchronous to the three different time locations within a 3 ns temporal wave packet, as shown in Fig. 4(c). The FPGA also provides a variable gate delay to synchronize the full systems, and to identify the interference slots. We recorded the photon arrival times by varying the RF delay to the PM for a fixed gate delay. Sifted key generation and QBER measurements for both Type-A and Type-B approaches were obtained after integrating a TDC and a time-stamp module in the FPGA.

V. Results and Discussion

A sifted key was derived after counting the TDC output, combined with that from a time-stamp module.

TABLE I
Classification of Photon Counts

Phase pattern	C_{pq}	T_{start}	T_{stop}
$\{0, 0\}$	C_{00}	T_0	$T_0 + 2\Delta T$
	C_{01}	$--$	$--$
	C_{10}	T_1	$T_1 + 2\Delta T$
	C_{11}	$--$	$--$
$\{0, \pi\}$	C_{00}	T_0	$T_0 + \Delta T$
	C_{01}	$T_0 + \Delta T$	$T_0 + 2\Delta T$
	C_{10}	T_1	$T_1 + \Delta T$
	C_{11}	$T_1 + \Delta T$	$T_1 + 2\Delta T$
$\{\pi, 0\}$	C_{00}	$T_0 + \Delta T$	$T_0 + 2\Delta T$
	C_{01}	T_0	$T_0 + \Delta T$
	C_{10}	$T_1 + \Delta T$	$T_1 + 2\Delta T$
	C_{11}	T_1	$T_1 + \Delta T$
$\{\pi, \pi\}$	C_{00}	$--$	$--$
	C_{01}	T_0	$T_0 + 2\Delta T$
	C_{10}	$--$	$--$
	C_{11}	T_1	$T_1 + 2\Delta T$

A. Key Generation

A final key rate of 21 kbps and 10 kbps was achieved in the Type-B and Type-A superposition schemes, with a QBER of 0.17 and 0.21, respectively, over 30 km of optical fiber. By further optimizing the DLI bias voltage and the control parameters of the SPD, we were able to observe a QBER of 0.12, shown pictorially in Fig. 7(a), in the time-bin scheme.

With reference to Figs. 6(a) and (b), the QBER is defined as,

$$\text{QBER} = \frac{C_{01} + C_{10}}{C_{00} + C_{10} + C_{01} + C_{11}} \tag{4}$$

where

$$C_{\text{pq}} = \sum_{t=T_{\text{start}}}^{T_{\text{stop}}} c_t \tag{5}$$

represents the counts at the p^{th} port of the DLI, when Alice's transmitted raw key is q. T_{start} and T_{stop} are determined for each case from Table I , with $T_1 - T_0 = 10$ ns.

We recovered the sifted key and extracted the QBER by directly comparing the sender's keys with the receiver's. This approach was used to optimize the RF delay and appropriately insert a phase shift every 1 ns within the 3 ns optical pulse, using a fixed pattern of $\{0, \pi\}$. Although the phase pattern was fixed, with a low mean photon number, channel loss, and a detector efficiency $\eta \sim 0.1$, we only detect a random bit pattern after the delay line interferometer.

The QKD testbed was also used to investigate the effect of excess bias voltage, gate width and hold-off time on the dark count rate (DCR) and afterpulse noises of a gated InGaAs single-photon detector (SPD) [21]. This helped in improvising the QBER for all 4 possible phase modulation patterns. We achieved a QBER of 0.12 for a fixed phase pattern $\{0, \pi\}$, as shown in Fig. 7(a). Other patterns $\{0, 0\}$, $\{\pi, 0\}$ and $\{\pi, \pi\}$ yielded a QBER of 0.09, 0.14 and 0.27 respectively as shown in Fig. 8, while a random pattern yielded a minimum QBER of 0.17 as shown in Fig. 7(b).

The sifted key generation rate in our time-bin superposition DPS system with time-multiplexed configuration can be written as [22]

$$R_{\text{sifted}} = r_{\text{p}} \mu \eta T_L e^{(-r_{\text{p}} \mu \eta T_L \tau_{\text{H}})} \tag{6}$$

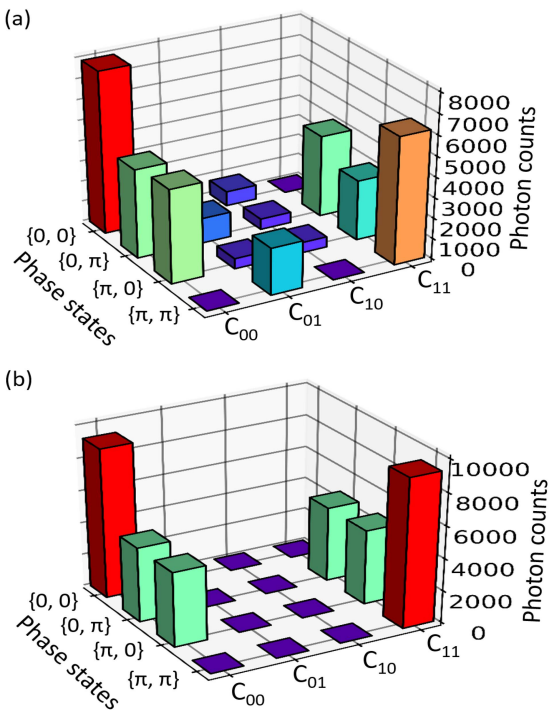

Fig. 8. Time-bin based differential-phase decoding by collecting photon arrival time for all four phase modulation states (a) experimental measurement (b) theoretical estimation.

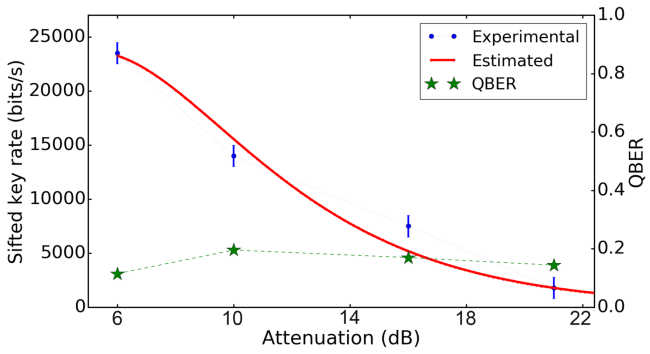

Fig. 9. Sifted key rate (estimated and experimental) and measured QBER as a function of channel length.

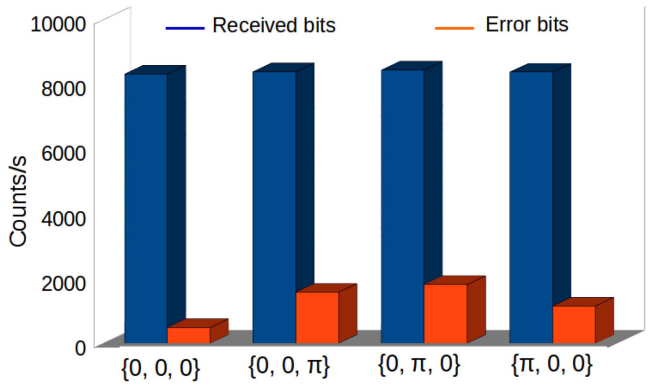

Fig. 10. Differential phase decoding in 8-state DPS-QKD. QBER for transmitted phase modulation states :$\{0, 0, 0\}$, $\{0, 0, \pi\}$, $\{0, \pi, 0\}$ and $\{\pi, 0, 0\}$ are 0.06, 0.20, 0.22 and 0.14 respectively.

TABLE II
VARIABLES USED IN SIFTED KEY RATE (6)

Variables	Description
r_{p}	Pulse repetition rate
α	Attenuation constant of a single mode fiber
μ	Mean photon number per pulse
T_L	$10^{-(\frac{\alpha L + I_L}{10})}$ (overall transmission efficiency of quantum channel)
η	Detection efficiency of SPD
T_{hold}	Hold-off time of SPD

TABLE III
POTENTIAL SOURCES OF ERRORS IN QKD TEST-BED, WITH A RANDOM BIT PATTERN

Description	Source	Error contribution (%)	
		FSR 1 GHz	FSR 2.5 GHz
Dark count rate (DCR)	SPD	0.33	0.33
Afterpulse effect	SPD	1.5	1.5
Extinction ratio	IM	1.6	1.6
Timing jitter	SPD	5.0	12.5
Imperfect visibility	DLI	4.0	2.0
Rise/fall time of PM pattern*	PM	2.1	5.25
Total error		14.5	23.2

* From data sheet.

where the variables used are defined in Table II.

T_L consists of fiber loss due to attenuation ($\alpha \approx 0.2$ dB/km) and the net insertion loss (I_L) of the DLI and coupler. Referring to (6), the values of r_{p}, η and τ_{H} are 31.25 Mbps, 10% and 10 μs respectively. The exponential term in (6) approaches 1 for a transmitted pulse rate of 31.25 Mbps, with a hold-off time of 10 μs, and R_{sifted} decreases linearly with distance. However, the exponent becomes significant for higher transmitted pulse rates, typically $r_{\mathrm{p}} > 1$ Gbps.

As we observe in Fig. 9, the experimental data fits well to (6), and we estimate $\mu \approx 0.34$. At a fiber length of 30 km, we achieved a sifted key generation rate of 21 kbps with a QBER of 11.5 %. We then extended our experiment to 105 km of fiber, and observed the sifted key rate drop to about 2 kbps with a QBER of 14.4 %, as shown in Fig. 9.

We further extended our 4-state DPS experiments to realize 8-state DPS, with a DLI having free spectral range of 2.5 GHz. The phase modulation transition rate was enhanced from 1 GHz to 2.5 GHz within a photon wave packet of width 1.6 ns, where each time-bin size is 0.4 ns. Based on the photon arrival time within 1.2 ns, the QBER was calculated for various phase modulation states, as shown in Fig. 10.

B. Temporal Filtering of Time-Stamps

After identification of the optimized gate and RF delay, we introduce a guard window between time-bins at the output state of Bob's set-up [23]. In temporal filtering, while we discard the time-stamps collected at the selected guard time, we lose a fraction of bits in sifted keys. However, this method reduces the QBER of a system [24], but at a cost of a reduced sifted key rate, as shown in Fig. 11(a) and (b). Table III lists the source of errors, contributing in QBER for our QKD test-bed. Error due

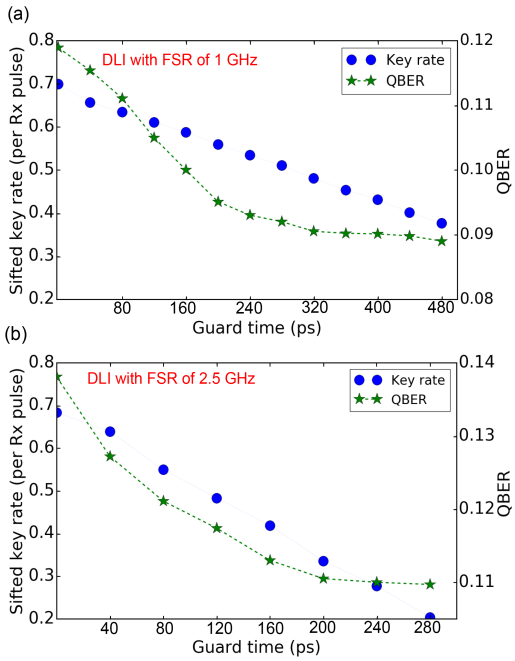

Fig. 11. Effect of temporal filtering on sifted key rate and QBER, (a) with DLI of FSR 1 GHz, and $\{0, \pi\}$ (b) with DLI of FSR 2.5 GHz, and $\{\pi, 0, 0\}$. With a higher guard time the QBER reduces, but at a cost of reduced sifted key rate per detection at the receiver (R_x).

to DCR, afterpulse probability and timing jitter were estimated from our previous work on gated SPD characterization [21].

The interferometric visibility (V) of two DLI with FSR of 1 GHz and 2.5 GHz are 92% and 96% respectively. The QBER introduced into the system due to V is $(1 - V)/2$.

It is possible to implement DPS-QKD by using coherent light and an IM with high extinction, such that the photons are in a superposition of temporal pulses [19]. The gap between transmitted pulses would act as a temporal guard band against electronic jitter in the phase modulator. However, as we attempt to increase the transmitted raw key rate, the separation between pulses decreases, eventually posing stricter constraints on the electronic drivers for the IM and PM. Consequently the QBER increases significantly. Under such a scenario, we find that it is easier to implement a temporal guard band while post-processing time-stamps at the receiver, during sifting.

To further validate this idea, we ran experiments with fixed bit patterns on each DLI. For a guard time of 200 ps, 20 % key bits are discarded, while the QBER is reduced from 0.12 to 0.09 in a system with a DLI of FSR 1 GHz, as shown in Fig. 11(a). For a DLI with 2.5 GHz FSR, we discard 20 % key bits, to reduce QBER from 0.14 to 0.12, as shown in Fig. 11(b). The reduction in QBER for a larger FSR is only marginal. This highlights a challenge of moving to a higher raw key rate and a DLI with a higher FSR, although we did find that the 2.5 GHz DLI did not require any active stabilization over even an hour of experimentation.

After estimating and optimizing QBER, we followed error correction and privacy amplification to generate secure keys. However, our focus is on QBER measurement and sifted key generation, hence error correction [25] and privacy amplification are not discussed in this paper.

TABLE IV
DECOY STATE IMPLEMENTATIONS [26], [27], [28]

Author, Year	Protocol	Encoding scheme	Channel length	Key rate bits/s
Frohlich et al., 2017	BB84	Phase	240 km	8.4
Boaron et al., 2018	Simplified BB84	Time-bin	421 km	6.5
Yuan et al., 2018	BB84 variant	Phase	10 km	13.7 M

TABLE V
MEASUREMENT-DEVICE-INDEPENDENT (MDI) QKD IMPLEMENTATIONS [29], [30], [31], [32], [33], [34], [35], [36]

Author, Year	Protocol	Encoding scheme	Channel length	Key rate bits/s
Yin et al., 2016	Decoy state MDI	Time-bin	404 km	0.00032
Tang et al., 2016	BB84	Polarisation	40 km	10
Comandar et al., 2016	BB84	Polarisation	102 km	4.6 K
Wang et al., 2016	RFI†	Time-bin	20 km	0.0063
Valivarthi et al., 2017	BB84	Time-bin	80 km	100
Liu et al., 2019	BB84	Time-bin	160 km	2.6
Wei et al., 2020	Asymmetric MDI	Polarization	180 km	31
Zhou, et al., 2021	RFI†	Time-bin	200 km	1

† Reference-frame-independent.

TABLE VI
TWIN-FIELD (TF) QKD IMPLEMENTATIONS [37], [38], [39], [40], [41], [42], [43]

Author, Year	Protocol	Encoding scheme	Channel length	Key rate bits/s
Minder et al., 2019	TF	Phase	90.8 dB	0.045
Wang et al., 2019	SNS-TF††	Time-bin	300 km	2.01 K
Liu et al., 2019	TF	Time-bin	300 km	39.2
Zhong et al., 2019	TF	Phase	55.1 dB	25.6
Fang et al, 2020	TF	Phase	502 km	0.118
Liu, Hui, et al, 2021	SNS-TF††	Time-bin	428 km	3.36
Wang, et al, 2021	TF	Phase	830 km	0.01

†† Sending-or-not-sending twin-field.

VI. CONCLUSION AND PERSPECTIVES

We have presented two different experimental approaches to generate time-bin superposition states: Type-A and Type-B, to realize a 4-state DPS-QKD experiment over a 105 km quantum channel. We observe that the Type-B approach has less stringent requirements on the intensity modulator, needs only a high quality phase modulator, and can be easily extended to an M-state DPS-QKD system implemented on a Si-photonics platform. Using commercial off-the-shelf components, and after optimization of various parameters, we achieved a sifted key rate of around 21 kbps with a QBER of 0.12 over 30 km of fiber. We then extended the Type-B system to 105 km of optical fibre, and achieved a sifted key rate of 2 kbps while maintaining a QBER of 0.14. The QBER was reduced back to 0.12 when we applied a temporal guard band during key sifting. Further increases in sifted key rate are limited by the timing jitter of the electronics, as the jitter becomes a larger fraction of the path delay at Bob's DLI.

APPENDIX A

Tables IV–VII provide a quick summary of key rates and channel lengths for a few recent implementations of QKD.

TABLE VII
CONTINUOUS VARIABLE-QKD [44], [45], [46]

Author, Year	Protocol	Encoding scheme	Channel length	Key rate bits/s
Wang et al., 2017	CV	Gaussian modulation	50 km	700
Zhang et al., 2019	CV	Gaussian modulation	50 km	5800
Zhang et al., 2020	CV	Gaussian modulation	202.8 km	6.2

REFERENCES

[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Rev. Modern Phys.*, vol. 74, no. 1, 2002, Art. no. 145.

[2] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Theor. Comput. Sci.*, vol. 560, pp. 7–11, 2014.

[3] Y. Liu et al., "Decoy-state quantum key distribution with polarized photons over 200 km," *Opt. Exp.*, vol. 18, no. 8, pp. 8587–8594, 2010.

[4] D. Stucki, S. Fasel, N. Gisin, Y. Thoma, and H. Zbinden, "Coherent one-way quantum key distribution," in *SPIE Photon Counting Applications, Quantum Optics, and Quantum Cryptography*. vol. 6583. Bellingham, WA, USA: SPIE, 2007, Art. no. 65830L.

[5] A. K. Ekert, "Quantum cryptography based on Bell's theorem," *Phys. Rev. Lett.*, vol. 67, no. 6, 1991, Art. no. 661.

[6] K. Inoue, E. Waks, and Y. Yamamoto, "Differential phase shift quantum key distribution," *Phys. Rev. Lett.*, vol. 89, no. 3, 2002, Art. no. 037902.

[7] S. Wang et al., "Field and long-term demonstration of a wide area quantum key distribution network," *Opt. Exp.*, vol. 22, no. 18, pp. 21739–21756, 2014.

[8] K. Inoue and T. Honjo, "Robustness of differential-phase-shift quantum key distribution against photon-number-splitting attack," *Phys. Rev. A*, vol. 71, no. 4, 2005, Art. no. 042305.

[9] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, "Experimental quantum cryptography," *J. Cryptol.*, vol. 5, no. 1, pp. 3–28, 1992.

[10] E. Waks, H. Takesue, and Y. Yamamoto, "Security of differential-phase-shift quantum key distribution against individual attacks," *Phys. Rev. A*, vol. 73, no. 1, 2006, Art. no. 012344.

[11] K. Wen, K. Tamaki, and Y. Yamamoto, "Unconditional security of single-photon differential phase shift quantum key distribution," *Phys. Rev. Lett.*, vol. 103, no. 17, 2009, Art. no. 170503.

[12] Y. Hui, Z. Shi-Liang, and D. Sheng-Wang, "Efficient phase-encoding quantum key generation with narrow-band single photons," *Chin. Phys. Lett.*, vol. 28, no. 7, 2011, Art. no. 070307.

[13] C. Liu et al., "Differential-phase-shift quantum key distribution using heralded narrow-band single photons," *Opt. Exp.*, vol. 21, no. 8, pp. 9505–9513, 2013.

[14] A. Boaron et al., "Simple 2.5 GHz time-bin quantum key distribution," *Appl. Phys. Lett.*, vol. 112, no. 17, 2018, Art. no. 171108.

[15] I. Vagniluca et al., "Efficient time-bin encoding for practical high-dimensional quantum key distribution," *Phys. Rev. Appl.*, vol. 14, no. 1, 2020, Art. no. 014051.

[16] L. Dellantonio, A. S. Sørensen, and D. Bacco, "High-dimensional measurement-device-independent quantum key distribution on two-dimensional subspaces," *Phys. Rev. A*, vol. 98, no. 6, 2018, Art. no. 062301.

[17] J.-Y. Guan et al., "Experimental passive round-robin differential phase-shift quantum key distribution," *Phys. Rev. Lett.*, vol. 114, no. 18, 2015, Art. no. 180502.

[18] W. Qu, H. Liu, J. Wang, and H. Ma, "Adjustable round-pulse time delayer for round-robin differential phase-shift quantum key distribution," *Opt. Commun.*, vol. 448, pp. 43–47, 2019.

[19] K. Inoue, E. Waks, and Y. Yamamoto, "Differential-phase-shift quantum key distribution using coherent light," *Phys. Rev. A*, vol. 68, no. 2, 2003, Art. no. 022317.

[20] S. K. Ranu, G. K. Shaw, A. Prabhakar, and P. Mandayam, "Security with 3-pulse differential phase shift quantum key distribution," in *Proc. IEEE Workshop Recent Adv. Photon.*, 2017, pp. 1–7.

[21] G. Shaw, S. Sridharan, and A. Prabhakar, "Gated InGaAs detector characterization with sub-picosecond weak coherent pulses," *Optik*, vol. 250, 2022, Art. no. 168280.

[22] E. Diamanti, H. Takesue, C. Langrock, M. Fejer, and Y. Yamamoto, "100 km differential phase shift quantum key distribution experiment with low jitter up-conversion detectors," *Opt. Exp.*, vol. 14, no. 26, pp. 13073–13082, 2006.

[23] G. K. Shaw, S. Sridharan, and A. Prabhakar, "Optimal temporal filtering for COW-QKD," in *Proc. IEEE Int. Conf. Signal Process. Commun.*, 2022, pp. 1–4.

[24] T. Kupko et al., "Tools for the performance optimization of single-photon quantum key distribution," *NPJ Quantum Inf.*, vol. 6, no. 1, pp. 1–8, 2020.

[25] A. K. Pradhan, A. Thangaraj, and A. Subramanian, "Construction of near-capacity protograph LDPC code sequences with block-error thresholds," *IEEE Trans. Commun.*, vol. 64, no. 1, pp. 27–37, Jan. 2015.

[26] A. Boaron et al., "Secure quantum key distribution over 421 km of optical fiber," *Phys. Rev. Lett.*, vol. 121, no. 19, 2018, Art. no. 190502.

[27] Z. Yuan et al., "10-mb/s quantum key distribution," *J. Lightw. Technol.*, vol. 36, no. 16, pp. 3427–3433, Aug. 2018.

[28] B. Fröhlich et al., "Long-distance quantum key distribution secure against coherent attacks," *Optica*, vol. 4, no. 1, pp. 163–167, 2017.

[29] H.-L. Yin et al., "Measurement-device-independent quantum key distribution over a 404 km optical fiber," *Phys. Rev. Lett.*, vol. 117, no. 19, 2016, Art. no. 190501.

[30] Z. Tang, K. Wei, O. Bedroya, L. Qian, and H.-K. Lo, "Experimental measurement-device-independent quantum key distribution with imperfect sources," *Phys. Rev. A*, vol. 93, no. 4, 2016, Art. no. 042308.

[31] L. Comandar et al., "Quantum key distribution without detector vulnerabilities using optically seeded lasers," *Nature Photon.*, vol. 10, no. 5, 2016, Art. no. 312.

[32] C. Wang, Z.-Q. Yin, S. Wang, W. Chen, G.-C. Guo, and Z.-F. Han, "Measurement-device-independent quantum key distribution robust against environmental disturbances," *Optica*, vol. 4, no. 9, pp. 1016–1023, 2017.

[33] R. Valivarthi et al., "A cost-effective measurement-device-independent quantum key distribution system for quantum networks," *Quantum Sci. Technol.*, vol. 2, no. 4, 2017, Art. no. 04LT01.

[34] H. Liu et al., "Experimental demonstration of high-rate measurement-device-independent quantum key distribution over asymmetric channels," *Phys. Rev. Lett.*, vol. 122, no. 16, 2019, Art. no. 160501.

[35] K. Wei et al., "High-speed measurement-device-independent quantum key distribution with integrated silicon photonics," *Phys. Rev. X*, vol. 10, no. 3, 2020, Art. no. 031030.

[36] X.-Y. Zhou et al., "Reference-frame-independent measurement-device-independent quantum key distribution over 200 km of optical fiber," *Phys. Rev. Appl.*, vol. 15, no. 6, 2021, Art. no. 064016.

[37] M. Minder et al., "Experimental quantum key distribution beyond the repeaterless secret key capacity," *Nature Photon.*, vol. 13, no. 5, pp. 334–338, 2019.

[38] S. Wang et al., "Beating the fundamental rate-distance limit in a proof-of-principle quantum key distribution system," *Phys. Rev. X*, vol. 9, no. 2, 2019, Art. no. 021046.

[39] Y. Liu et al., "Experimental twin-field quantum key distribution through sending or not sending," *Phys. Rev. Lett.*, vol. 123, no. 10, 2019, Art. no. 100505.

[40] X. Zhong, J. Hu, M. Curty, L. Qian, and H.-K. Lo, "Proof-of-principle experimental demonstration of twin-field type quantum key distribution," *Phys. Rev. Lett.*, vol. 123, no. 10, 2019, Art. no. 100506.

[41] X.-T. Fang et al., "Implementation of quantum key distribution surpassing the linear rate-transmittance bound," *Nature Photon.*, vol. 14, pp. 422–425, 2020.

[42] H. Liu et al., "Field test of twin-field quantum key distribution through sending-or-not-sending over 428 km," *Phys. Rev. Lett.*, vol. 126, no. 25, 2021, Art. no. 250502.

[43] S. Wang et al., "Twin-field quantum key distribution over 830-km fibre," *Nature Photon.*, vol. 16, pp. 154–161, 2022.

[44] X. Wang, W. Liu, P. Wang, and Y. Li, "Experimental study on all-fiber-based unidimensional continuous-variable quantum key distribution," *Phys. Rev. A*, vol. 95, no. 6, 2017, Art. no. 062330.

[45] Y. Zhang et al., "Continuous-variable QKD over 50 km commercial fiber," *Quantum Sci. Technol.*, vol. 4, no. 3, 2019, Art. no. 035006.

[46] Y. Zhang et al., "Long-distance continuous-variable quantum key distribution over 202.81 km of fiber," *Phys. Rev. Lett.*, vol. 125, no. 1, 2020, Art. no. 010502.