Equivalence of space and time-bins in DPS-QKD

G K Shaw[1], S K Ranu[1,2], S Shyam[1], Foram S[1], P Mandayam[2], A Prabhakar[1]
[1]**Department of Electrical Engineering, Indian Institute of Technology Madras, Chennai, India.**
[2]**Deptartment of Physics, Indian Institute of Technology Madras, Chennai, India.**

Abstract: We set up differential phase shift quantum key distribution (DPS-QKD), over 105 km of single mode optical fiber, with a quantum bit error rate less than 15% at a secure key rate of 2 kbps. The testbed was used to investigate the effect of excess bias voltage and hold-off time on the temporal distribution of photons within a gate window of an InGaAs single-photon detector (SPD), and quantify the effects of after pulsing. The key generation efficiency, and security, in DPS-QKD improve with an increase in the number of path delays or time-bin superpositions.

1. Key generation in DPS-QKD

The sender (Alice) uses a photon in a superposition state, corresponding to either 3 spatial paths or temporal bins. In the temporal case, Alice uses a weak coherent source (WCS) with a pulse width of 3 ns, that we interpret as a single wave packet comprising of three time-bins of 1 ns each. Alice encodes her random key bit [0, 1] as a random phase [0, π] between $|a\rangle$ and $|b\rangle$, and $|b\rangle$ and $|c\rangle$, i.e. successive paths or time bins of the WCS, with mean photon number μ=0.2 (Fig. 1 (left))[1][2]. The phase encoded bits are then transmitted over a single mode optical fibre. Both path and time-bin implementations follow similar setups beyond the transmitter. We recovered the sifted key and extracted the QBER by directly comparing the sender's keys with the receiver's. 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. 1 (right).

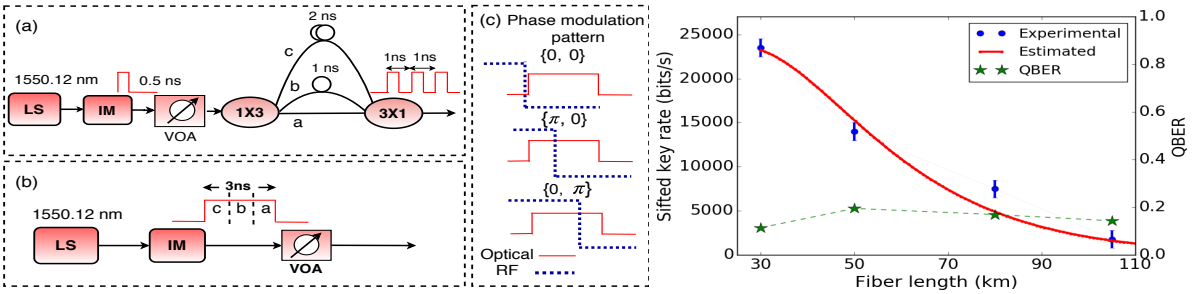

Fig. 1. Weak coherent sources for (a) spatial, and (b) time-bin superposition (c) phase modulation pattern, the sifted key and QBER were obtained for different lengths of single mode optical fiber

References

1. K. Inoue, E. Waks, and Y. Yamamoto, Differential phase shift quantum key distribution,Physical Review Letters,vol. 89, no. 3, p. 037902, 2002.

2. S. K. Ranu, G. K. Shaw, A. Prabhakar, and P. Mandayam,Security with 3-pulse differential phase shift quantum key distribution, in2017 IEEE Workshop on Recent Advances in Photonics (WRAP).IEEE, 2017, pp. 17.

Equivalence of space and time-bins in DPS-QKD

Gautam Shaw*, Shyam Sridharan*, Shashank Ranu†*, Foram Shingala*, Prabha Mandayam†, and Anil Prabhakar*
*Department of Electrical Engineering, IIT Madras, Chennai, India
†Department of Physics, IIT Madras, Chennai, India

***Abstract*—We set up differential phase shift quantum key distribution (DPS-QKD), over 105 km of single mode optical fiber, with a quantum bit error rate less than $15\,\%$ at a secure key rate of 2 kbps. The testbed was first used to investigate the effect of excess bias voltage and hold-off time on the temporal distribution of photons within a gate window of an InGaAs single-photon detector (SPD), and quantified the effects of after pulsing. The key generation efficiency, and security, in DPS-QKD improve with an increase in the number of path delays or time-bin superpositions. We finally demonstrate the implementation of superposition states using a time-bin approach, and establish an equivalence with the path-based superposition approach, thus yielding a simpler approach to implementing superposition states for use in DPS-QKD.**

***Index Terms*—Quantum key distribution; differential phase shift protocol; spatial superposition; time-bin superposition**

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, 2]. 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 [3–6]. Field demonstrations of QKD have mostly used discrete variables, and with some active stabilization to mitigate environmental fluctuations [7]. Appendix A provides the reader with a quick summary of key rates and channel lengths for a few recent implementations of QKD.

K. Inoue et. al proposed a differential phase-shift quantum key distribution (DPS-QKD) protocol, that is easy 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 was established under the assumption that Eve is restricted to individual attacks [10]. Conventional DPS-QKD was demonstrated with sifted key rates of 2 Mb/s and 166 bits/s over a 10 km and 100 km fiber respectively, using a low jitter frequency up-conversion single photon detector [11]. Shibata et al. demonstrated first long distance differential phase shift quantum key distribution (DPS-QKD) over a 336 km length of dispersion shifted fiber using weak coherent pulses (WCPs) and superconducting nanowire single-photon detectors [12].

The main security threat to such systems arises from the finite probability that some pulses contain more than one photon. Hence, the photon number splitting (PNS) attack by Eve severely limits the distance over which secure keys can be transmitted in such QKD systems. In a PNS attack, Eve performs a quantum non-demolition (QND) measurement on each WCP. Entangled photon pair based QKD schemes are robust against such attacks [13, 14]. But, such demonstrations of entanglement-based QKD suffer from a lower secure key rate (less than 1 bit/s) and are limited to shorter lengths of optical fibres. Continuous variable systems are harder to implement, but can use telecommunication grade components and provide security against general collective eavesdropping attacks [15–17].

The unconditional security of a single-photon source, with path superposition and a differential phase, yields an optimally secure key generation rate per pulse with a maximum achievable distance [18]. Thereafter, an efficient phase encoding quantum key generation scheme, with narrow band heralded photons, was proposed by Yan et al. [19]. The differential quadrature scheme, DQPS-QKD, uses four phases $\Phi = 0, \pi/2, \pi, 3\pi/2$ to generate four non-orthogonal states, analogous to the BB84 protocol [20]. The recently introduced round-robin differential phase-shift quantum key distribution (RR-DPS-QKD) scheme address the effects of environmental disturbances, and give us an upper bound on our tolerance to error rates with a bit error rate as high as 29% [21]. But such schemes requires the addition of optical switches and delays that make Bob's set-up more complex [22].

In this article, we aim to establish the equivalence between spatial and temporal generation of a superposition state, for use in a DPS-QKD system. In Sec. IV, we show that the two methods yield comparable key rates in kbps, with a QBER < 0.2. However, time-bins are defined electronically, and are significantly easier to generate. 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.

After-pulsing effects are an inherent limitation of a single photon detector (SPD) and have a considerable impact on high speed QKD systems [23]. This effect is associated with the lifetime of trapped carriers and determines the hold-off time after a successful detection [24]. In Sec. IV-A, we propose a characterization method for the after-pulsing probabilities using a picosecond mode locked fibre laser. These detector characterization experiments help us quantify the errors in our 4-state DPS implementation, with a resolution of 55 ps, and

Gautam Shaw is with the Department of Electrical Engineering, Indian Institute of Technology, Madras, e-mail: ee15d047@ee.iitm.ac.in.

better distinguish the photon arrival time-bins.

II. Experimental Setup

In the original proposal for DPS-QKD, a single photon is allowed to pass through a beam splitter, travel through different path delays and is recombined back to create a superposition state of the photon [6]. However, this scheme encounters beam splitter losses and reduces the secure key rate. With a path superposition of N-paths, and a relative phase of $\{0, \pi\}$ between paths, the photon can be in a superposition of 2^{N-1} states. Similar states can be also achieved with time-bin superposition by adding a relative phase at $N-1$ locations within a single pulse. In this article, we define 2^{N-1} as M, and hence, refer to the 3-pulse DPS-QKD as a 4-state system, to allow us to describe the creation of superposition states by temporal phase modulation [19].

We describe our experiments with 4-state DPS-QKD, using spatial and time-bin superposition of a weak coherent source, as shown in Fig. 1. The time-bin superposition scheme is 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. This percentage error increases to 50% when 4-state DPS is extended to M-state DPS [25].

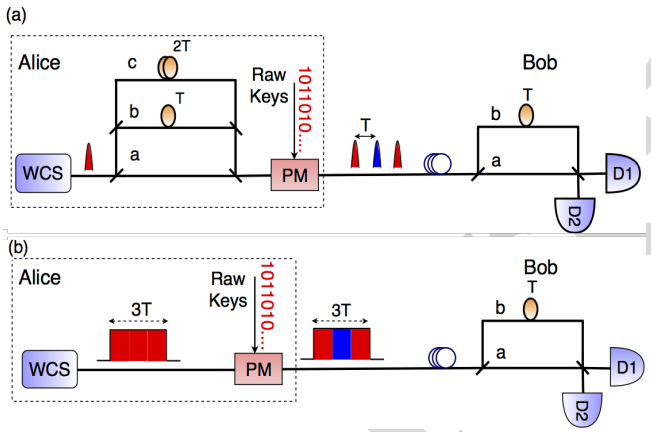

Fig. 1: 4-state DPS-QKD schemes using (a) spatial and (b) time-bin superposition with a weak coherent source. WCS: Weak coherent source, PM: phase modulator, T: time, D1 and D2: single photon detectors.

The methodology used to implement a weak coherent source (WCS) is described along with the rest of our experimental setup in Sec. IV-B.

III. Key generation in DPS-QKD

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

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

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

This superposition of 3 time-bins 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. This 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 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 higher error rate in 4-state DPS makes it easier to detect Eve's presence.

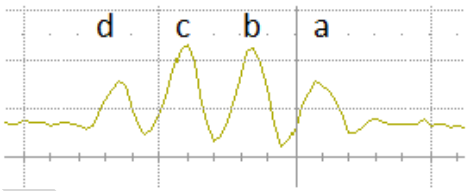

Fig. 2: Photodetector output after Alice's path superposition and Bob's DLI, captured with a diode laser source. The key is generated by the interference in time-bins b and c.

A photon is detected in the first (last) time slot if it travels through first (third) path in Alice's 3 pulse set-up and shorter (longer) arm in Bob's DLI. The probability of detection of a photon in the 1st and 4th time slot is $\frac{1}{6}+\frac{1}{6} = \frac{1}{3}$. Thus, the sifted key rate (R_{sifted}) is equal to $\frac{2}{3}$. Similarly, if Alice transmits n photons where each photon is in a superposition of N time-bins, only $n\left[\frac{N-1}{N}\right]$ photons contribute to the final keys, and hence the sifted key rate (R_{Sifted}) is equal to $\frac{N-1}{N}$ [25]. For a higher value of N, the sifted key rate converges towards 1 as shown in Fig. 3. We also show the dependence of secure key rate on the number of delays/time-bins in Alice's setup. The secure key rate is given as [11]

$$R_{\text{sec}} = R_{\text{sifted}}\big(\tau - f(e)h(e)\big), \quad (3)$$

where τ is the shrinking factor, e is the error rate, $f(e)$ captures the inefficiency of the error correcting code, and $h(e)$ is the binary Shannon entropy. The error rate depends upon dark counts and other system imperfections. τ captures Eve's knowledge of the key. In this paper, we assume Eve's attack to be limited to IR and beamsplitter attacks only. Increasing N changes the efficacy of the attacks, thus making τ a function of N [25]. 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 spatially using passive beam splitters (or beam

combiners). However, passive beam splitters have insertion losses and the sifted key rate is reduced by a factor of N, thus making the implementation inefficient. The optimal number of paths in such a scenario was determined to be 3 paths, or a superposition of 3 time-bin states [25]. As described by (2), these states form 4 non-orthogonal states that Alice uses to transmit the key. Keeping in mind the ease of implementing time-bin superposition, we advocate temporal bins using phase modulation, over different spatial paths. This would allows us to use $N > 3$ and obtain a higher sifted key rate, as seen in Fig. 3.

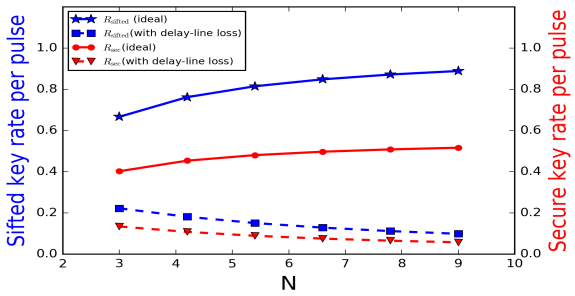

Fig. 3: Estimates for the sifted and secure key rate for M-state DPS-QKD.

IV. Experimental Results

A. Characterization of single photon detectors

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.

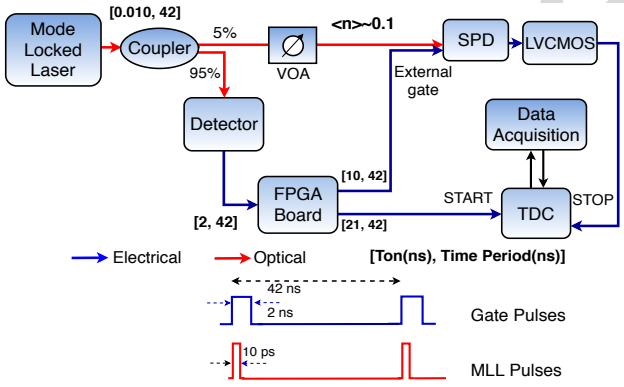

Fig. 4: After pulsing characterization set-up.

Short coherent pulses, generated from a 1555 nm mode locked fiber laser, were attenuated to a mean photon number $\mu \sim 0.1$ and allowed to fall on a gated SPD as shown in Fig. 4. A small fraction (5%) of the laser pulse was sent to a 5 GHz photodetector using an optical splitter, and used to trigger a field programmable gate array (FPGA) board synchronous with the mode locked laser (MLL) pulses. The FPGA board was programmed with electronic delays and used to adjust the time delay of gate pulses relative to the arrival

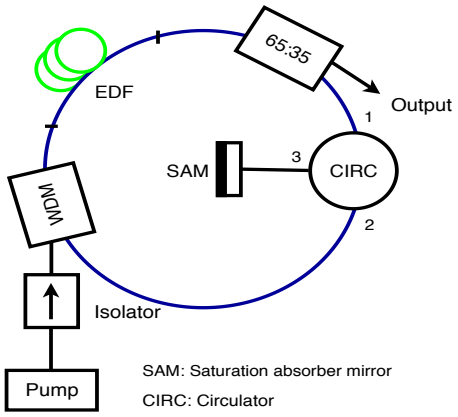

Fig. 5: Schematic of a mode locked fibre laser [25].

time of a photon at the SPD. The SPD was then gated with a 2 ns electrical pulse. By adjusting the timing of the arrival photon, relative to the gate pulse, we were able to collect the distribution of photons within the gate width. A time to digital converter, the TDC7200 from Texas Instruments, interfaced with a TIVA Launchpad micro-controller, was used to digitize the timing instants of photon arrival at the SPD, thus yielding the temporal photon distribution within a gate pulse duration. We swept the gate pulse, of various widths, in steps of 200 ps through the MLL pulse repetition time of 42 ns and measured the photon counts per second incident on the SPD.

Fig. 6 captures the uneven distribution of photon counts corresponding to the unequal rise time and fall times of the gate pulse. For a gate width of 2 ns, the photon counts/s are a maximum for a gate delay of 13.2 ns. The fall time in each data set is longer than the rise time, seen clearly in the plots for a 2.2-2.5 ns gate width. The fall times are also quantified in Fig. 7, with the minimum fall time of 0.85 ns observed for a gate width of 2 ns. The longer fall times for larger gate widths is attributed to after-pulses that occur after the photon has hit the SPD, while there is no significant change in the rise times. However, the plots in Fig. 6 and Fig. 7 don't capture the statistics of photon arrival within the duration of the gate. Better resolution was achieved by using the TDC7200, interfaced with an Arduino board and the acquisition system shown in Fig. 4.

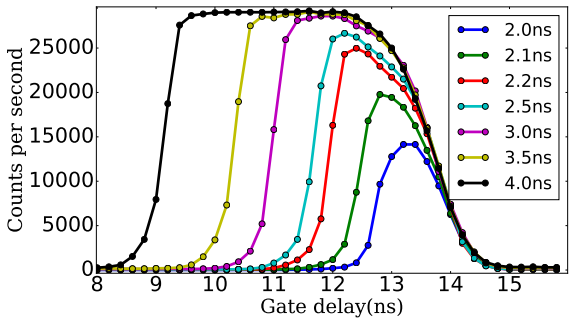

Fig. 6: After pulsing effect with various gate width.

We achieved good temporal resolution by monitoring the

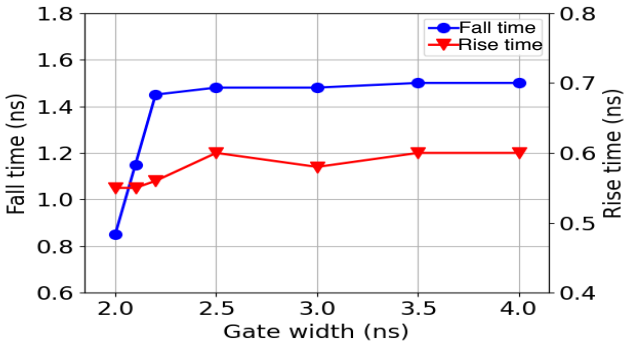

Fig. 7: Effects of after pulsing extracted from the trailing edge of the gate in Fig. 6, are observed as longer fall times for gate widths greater than 2 ns.

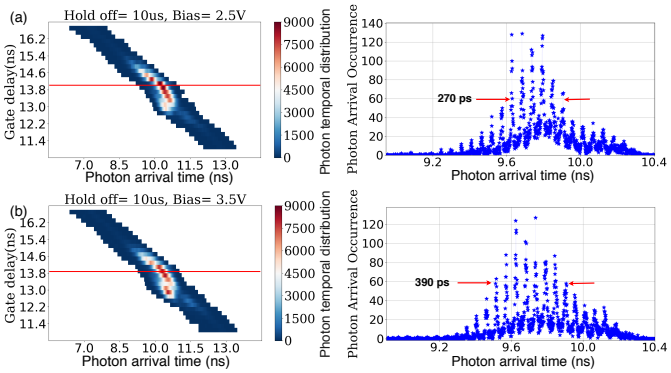

Fig. 8: Effect of bias voltage on photon distribution for an excess bias of (a) 2.5 V, and (b) 3.5 V.

time stamps associated with the clicks recorded at the SPD. The TDC start pulse is synchronized to the gate pulse and the SPD generates the TDC stop pulse. The gate delay was swept in steps of 200 ps, and the arrival time of photons were collected for each gate delay.

Before conducting the after-pulsing experiment, we measured dark counts of 300 counts/s with an internal gate width of 2 ns, at a repetition rate of 120 MHz or an interval of 8.3 ns between consecutive gate pulses. At a longer gate interval of 42 ns, the dark counts reduce to 100 counts/s. There is thus a trade-off between our ability to detect incoming photons, and becoming susceptible to higher after-pulsing probabilities. Consequently, a high raw key rate does not guarantee a higher sifted key rate. Although the total counts/s decrease as we reduce the gate width, we prefer the shortest gate pulse of 2 ns as it yields fewer false detections.

Another parameter is the excess bias voltage (V_{EX}), defined as the difference of the reverse bias voltage (V_{R}) and the breakdown voltage (V_{BR}),

$$V_{\mathrm{EX}} = V_{\mathrm{R}} - V_{\mathrm{BR}} \tag{4}$$

To investigate the effect of excess bias voltage on an SPD, we increase V_{EX} from 2.0 V to 4.0 V, in steps of 0.5 V, keeping the hold-off time at 10 μs, and maintaining a SPD temperature of 233 K. Fig. 8 represents the photon distribution within a 2 ns gate width for two excess bias voltage 2.5 V and 3.5 V. The distributions have a full width at half maximum (FWHM) of 270 ps and 390 ps for 2.5 V and 3.5 V respectively. However, keeping $V_{\mathrm{EX}} \approx 2.5$ V, while changing the hold-off time (T_{H}) from 10 μs to 20 μs doesn't effect the photon arrival time within a 2 ns gate. The peaks in the distribution within a gate width are a combination of timing jitter and quantization within the TDC. However, a higher V_{EX} clearly causes a wider timing distribution. For our 4-state DPS-QKD experiment, we fixed V_{EX} at 2.5 V and $T_{\mathrm{H}} = 10\,\mu$s.

B. DPS-QKD implementation

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 16 ns, are applied to a 3 GHz intensity modulator (IM). The bias voltage to the IM needed to be optimized, to get a modulation extinction of more than 10 dB. The resultant optical pulses were then attenuated, using a variable optical attenuator (VOA), to a mean photon number $\mu \sim 0.1$. The photons were then sent directly to a gated SPD and we observed 31 K-counts/s when the gate window was synchronized with the photon arrival time. This reduced to around 2.5 K-counts/s when the gate was out of sync with the arrival of the photons.

Two different source configurations for path and time-bin superposition, shown in Fig. 9, were then used in the DPS-QKD experimental set-up shown in Fig. 10. In Fig. 9(a), weak coherent pulses are passed through 1×3 and 3×1 beam splitter-coupler combination so that photons coming out from 3×1 coupler are in superposition of three paths before being passed through the phase modulator (PM), shown in Fig. 10. In Fig. 9(b), a 3 ns pulse coming out of the intensity modulator (IM) is attenuated and acts as a source. Phase modulation can be introduced on this pulse, as shown in Fig. 9(c).

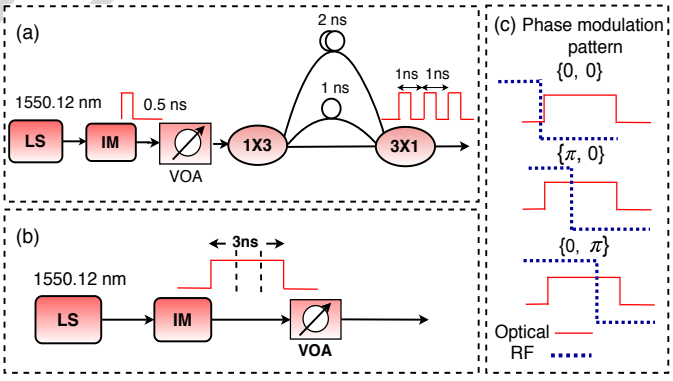

Fig. 9: Weak coherent sources for (a) spatial, and (b) time-bin superposition. LS:laser source, IM: intensity modulator, VOA: variable optical attenuator. (c) Phase modulation pattern

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

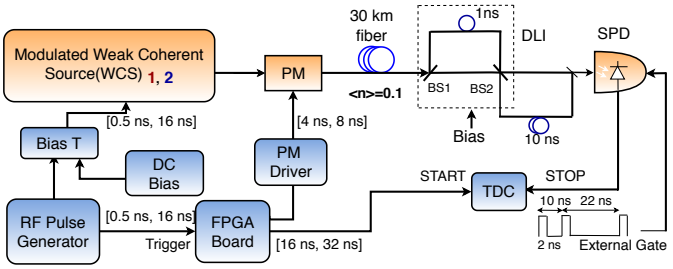

Fig. 10: 3 pulse DPS-QKD experimental set-up.

DLI. A fiber delay of 10 ns was added at one of the output port of the DLI. 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. Rather, using a single detector has the advantage of providing a equal sensitivity on both constructive and destructive interference ports of the DLI.

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 $\{0, 0\}$, $\{\pi, 0\}$ and $\{0, \pi\}$ 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. 9(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 space and time multiplexed schemes 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. A final key rate of 21 kbps and 10 kbps was achieved in the time-bin superposition and path superposition schemes, with a QBER of 17 % and 21 % respectively over 30 km of optical fiber. By optimizing the DLI bias voltage and the control parameters of the SPD, we were able to observe a QBER of 11.5 %, shown pictorially in Fig. 13. This is mostly attributed to imperfect interferometry (DLI visibility of 83 %). Other factors that contribute to the QBER are the rise time of the phase modulating signal (approximately 270 ps), bandwidth of intensity modulator (3 GHz) and the DLI bias voltage.

With reference to Figs. 11 and 12, the QBER is defined as,

$$\text{QBER} = \frac{C_{01} + C_{10}}{C_{00} + C_{10} + C_{01} + C_{11}}, \tag{5}$$

where $C_{01}(C_{10})$ represents the total photon counts at constructive port (destructive port) of DLI, when Alice's transmitted raw key is '1'('0').

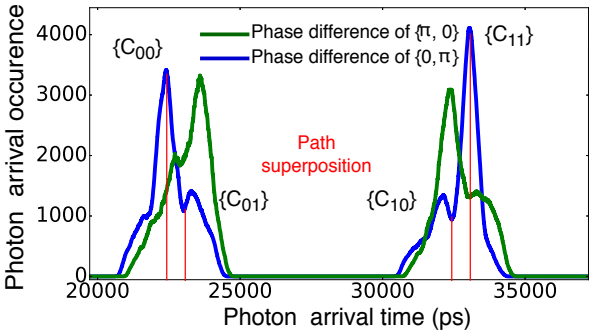

Fig. 11: Photon arrival time distribution for path superposition 4-state DPS-QKD

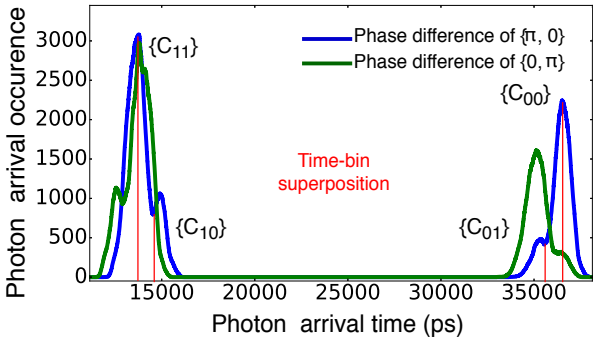

Fig. 12: Photon arrival time distribution for time-bin superposition 4-state DPS-QKD

We also 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.

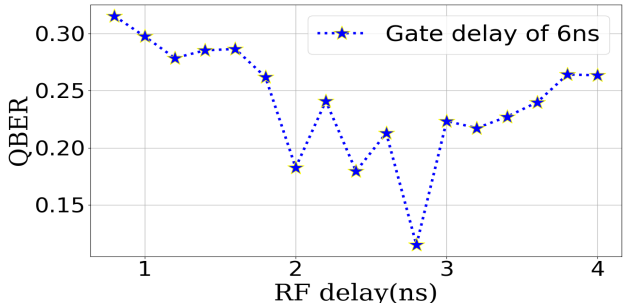

Fig. 13: Optimization of QBER by adjusting the timing of the applied phase.

The sifted key generation rate in our time-bin superposition DPS system can be written as [11]

$$R_{\text{sifted}} = \nu\mu\eta T_L e^{(-\nu\mu\eta T_L \tau_H)} \tag{6}$$

where ν, μ, $T_L = 10^{-(\frac{\alpha L + I_L}{10})}$, η and τ_{H} are pulse repetition rate, mean photon number per pulse, overall transmission efficiency of quantum channel, detector efficiency and detector hold-off time, respectively. The overall transmission efficiency of quantum channel consists of fiber loss due to attenuation (typically, attenuation constant of single mode fiber is 0.2 dB/km) and insertion loss (I_L) of DLI and coupler. Referring to (6), the values of ν, η and τ_{H} are 62.5 Mbps, 10% and 10 μs respectively. The exponential term in (6) approaches 1 for a transmitted pulse rate of 62.5 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 $\nu > 1$ Gbps. As we observe in Fig. 14, the experimental data fits well to (6), and we estimate $\mu \approx 0.17$. 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. 14.

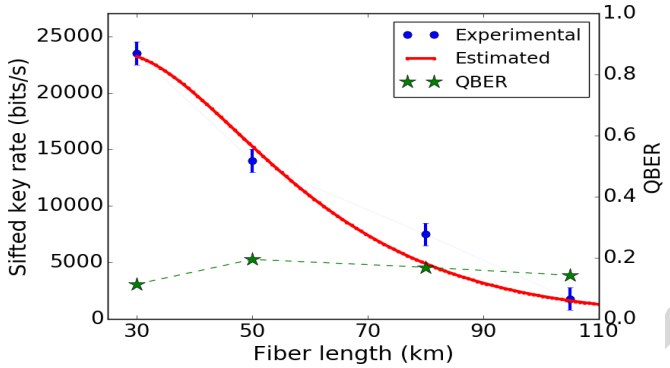

Fig. 14: Sifted key rate (estimated and experimental) and measured QBER as a function of channel length

VI. Conclusion and Perspectives

We have presented two different experimental approaches (a) spatial superposition and (b) time-bin superposition, to realize a 4-state DPS-QKD over a 105 km quantum channel. A prior knowledge of photon distribution within the temporal gate width was essential to realize the time-bin superposition a 4-state DPS-QKD system. We used ultra-short weak coherent pulses, from a MLL, to investigate the effect of the SPD settings, bias voltage and detector hold-off time, on the temporal distribution of photon detections within the gate width. After optimization of various parameters, we achieved a sifted key rate of around 21 kbps with QBER of 11.5% over 30 km of fiber. We then extended our time-bin superposition based DPS-QKD system to 105 km of optical fibre, and achieved a sifted key rate of 2 kbps while maintaining QBER of 14.4%. We observe that the time-bin superposition scheme is more efficient and easier to implement and can be extended to an M-state DPS-QKD system. A natural extension of this work is to use time-bin superposition for round-robin DPS-QKD.

Acknowledgment

This work was supported by Ministry of Human Resources and Development (MHRD) vide sanction no. 35-8/2017-TS. We are thankful to QuNu Labs, Bengaluru for initial support.

Appendix

TABLE I: Decoy state implementations [26–28]

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	13.7×10^6

TABLE II: MDI-QKD implementations [29–34]

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	Reference frame independent	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., 2019	Asymmetric MDI	Polarization	105 km	6.2 K

TABLE III: Twin field QKD implementations [35–39]

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

TABLE IV: Continuous variable-QKD [15–17]

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	5.8 K
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," *Reviews of Modern Physics*, vol. 74, no. 1, p. 145, 2002.

[2] C. H. Bennett and G. Brassard, "Quantum cryptography: public key distribution and coin tossing," 1984.

[3] Y. Liu, T.-Y. Chen, J. Wang, W.-Q. Cai, X. Wan, L.-K. Chen, J.-H. Wang, S.-B. Liu, H. Liang, L. Yang *et al.*, "Decoy-state quantum key distribution with polarized photons over 200 km," *Optics Express*, 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 *Photon Counting Applications, Quantum Optics, and Quantum Cryptography*, vol. 6583. International Society for Optics and Photonics, 2007, p. 65830L.

[5] A. K. Ekert, "Quantum cryptography based on bells theorem," *Physical Review Letters*, vol. 67, no. 6, p. 661, 1991.

[6] K. Inoue, E. Waks, and Y. Yamamoto, "Differential phase shift quantum key distribution," *Physical Review Letters*, vol. 89, no. 3, p. 037902, 2002.

[7] S. Wang, W. Chen, Z.-Q. Yin, H.-W. Li, D.-Y. He, Y.-H. Li, Z. Zhou, X.-T. Song, F.-Y. Li, D. Wang *et al.*, "Field and long-term demonstration of a wide area quantum key distribution network," *Optics express*, vol. 22, no. 18, pp. 21 739–21 756, 2014.

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

[9] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, "Experimental quantum cryptography," *Journal of Cryptology*, 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," *Physical Review A*, vol. 73, no. 1, p. 012344, 2006.

[11] 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," *Optics Express*, vol. 14, no. 26, pp. 13 073–13 082, 2006.

[12] H. Shibata, T. Honjo, and K. Shimizu, "Quantum key distribution over a 72 db channel loss using ultralow dark count superconducting single-photon detectors," *Optics letters*, vol. 39, no. 17, pp. 5078–5081, 2014.

[13] S. Barz, G. Cronenberg, A. Zeilinger, and P. Walther, "Heralded generation of entangled photon pairs," *Nature Photonics*, vol. 4, no. 8, p. 553, 2010.

[14] S.-K. Liao, H.-L. Yong, C. Liu, G.-L. Shentu, D.-D. Li, J. Lin, H. Dai, S.-Q. Zhao, B. Li, J.-Y. Guan *et al.*, "Long-distance free-space quantum key distribution in daylight towards inter-satellite communication," *Nature Photonics*, vol. 11, no. 8, p. 509, 2017.

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

[16] Y. Zhang, Z. Li, Z. Chen, C. Weedbrook, Y. Zhao, X. Wang, Y. Huang, C. Xu, X. Zhang, Z. Wang *et al.*, "Continuous-variable qkd over 50 km commercial fiber," *Quantum Science and Technology*, vol. 4, no. 3, p. 035006, 2019.

[17] Y.-C. Zhang, Z. Chen, S. Pirandola, X. Wang, C. Zhou, B. Chu, Y. Zhao, B. Xu, S. Yu, and H. Guo, "Long-distance continuous-variable quantum key distribution over 202.81 km fiber," *arXiv preprint arXiv:2001.02555*, 2020.

[18] K. Wen, K. Tamaki, and Y. Yamamoto, "Unconditional security of single-photon differential phase shift quantum key distribution," *Physical Review Letters*, vol. 103, no. 17, p. 170503, 2009.

[19] Y. Hui, Z. Shi-Liang, and D. Sheng-Wang, "Efficient phase-encoding quantum key generation with narrow-band single photons," *Chinese Physics Letters*, vol. 28, no. 7, p. 070307, 2011.

[20] S. Kawakami, T. Sasaki, and M. Koashi, "Security of the differential-quadrature-phase-shift quantum key distribution," *Phys. Rev. A*, vol. 94, p. 022332, Aug 2016. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.94.022332

[21] J.-Y. Guan, Z. Cao, Y. Liu, G.-L. Shen-Tu, J. S. Pelc, M. Fejer, C.-Z. Peng, X. Ma, Q. Zhang, and J.-W. Pan, "Experimental passive round-robin differential phase-shift quantum key distribution," *Physical review letters*, vol. 114, no. 18, p. 180502, 2015.

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

[23] G.-J. Fan-Yuan, C. Wang, S. Wang, Z.-Q. Yin, H. Liu, W. Chen, D.-Y. He, Z.-F. Han, and G.-C. Guo, "After-pulse analysis for quantum key distribution," *Physical Review Applied*, vol. 10, no. 6, p. 064032, 2018.

[24] J. Zhang, M. A. Itzler, H. Zbinden, and J.-W. Pan, "Advances in InGaAs/InP single-photon detector systems for quantum communication," *Light: Science & Applications*, vol. 4, no. 5, p. e286, 2015.

[25] S. K. Ranu, G. K. Shaw, A. Prabhakar, and P. Mandayam, "Security with 3-pulse differential phase shift quantum key distribution," in *2017 IEEE Workshop on Recent Advances in Photonics (WRAP)*. IEEE, 2017, pp. 1–7.

[26] A. Boaron, G. Boso, D. Rusca, C. Vulliez, C. Autebert, M. Caloz, M. Perrenoud, G. Gras, F. Bussières, M.-J. Li *et al.*, "Secure quantum key distribution over 421 km of optical fiber," *Physical review letters*, vol. 121, no. 19, p. 190502, 2018.

[27] Z. Yuan, A. Plews, R. Takahashi, K. Doi, W. Tam, A. Sharpe, A. Dixon, E. Lavelle, J. Dynes, A. Murakami *et al.*, "10-mb/s quantum key distribution," *Journal of Lightwave Technology*, vol. 36, no. 16, pp. 3427–3433, 2018.

[28] B. Fröhlich, M. Lucamarini, J. F. Dynes, L. C. Comandar, W. W.-S. Tam, A. Plews, A. W. Sharpe, Z. Yuan, and A. J. Shields, "Long-distance quantum key distribution secure against coherent attacks," *Optica*, vol. 4, no. 1, pp. 163–167, 2017.

[29] H.-L. Yin, T.-Y. Chen, Z.-W. Yu, H. Liu, L.-X. You, Y.-

H. Zhou, S.-J. Chen, Y. Mao, M.-Q. Huang, W.-J. Zhang *et al.*, "Measurement-device-independent quantum key distribution over a 404 km optical fiber," *Physical review letters*, vol. 117, no. 19, p. 190501, 2016.

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

[31] L. Comandar, M. Lucamarini, B. Fröhlich, J. Dynes, A. Sharpe, S.-B. Tam, Z. Yuan, R. Penty, and A. Shields, "Quantum key distribution without detector vulnerabilities using optically seeded lasers," *Nature Photonics*, vol. 10, no. 5, p. 312, 2016.

[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, Q. Zhou, C. John, F. Marsili, V. B. Verma, M. D. Shaw, S. W. Nam, D. Oblak, and W. Tittel, "A cost-effective measurement-device-independent quantum key distribution system for quantum networks," *Quantum Science and Technology*, vol. 2, no. 4, p. 04LT01, 2017.

[34] H. Liu, W. Wang, K. Wei, X.-T. Fang, L. Li, N.-L. Liu, H. Liang, S.-J. Zhang, W. Zhang, H. Li *et al.*, "Experimental demonstration of high-rate measurement-device-independent quantum key distribution over asymmetric channels," *Physical review letters*, vol. 122, no. 16, p. 160501, 2019.

[35] M. Minder, M. Pittaluga, G. Roberts, M. Lucamarini, J. Dynes, Z. Yuan, and A. Shields, "Experimental quantum key distribution beyond the repeaterless secret key capacity," *Nature Photonics*, vol. 13, no. 5, pp. 334–338, 2019.

[36] S. Wang, D.-Y. He, Z.-Q. Yin, F.-Y. Lu, C.-H. Cui, W. Chen, Z. Zhou, G.-C. Guo, and Z.-F. Han, "Beating the fundamental rate-distance limit in a proof-of-principle quantum key distribution system," *Physical Review X*, vol. 9, no. 2, p. 021046, 2019.

[37] Y. Liu, Z.-W. Yu, W. Zhang, J.-Y. Guan, J.-P. Chen, C. Zhang, X.-L. Hu, H. Li, C. Jiang, J. Lin *et al.*, "Experimental twin-field quantum key distribution through sending or not sending," *Physical Review Letters*, vol. 123, no. 10, p. 100505, 2019.

[38] X. Zhong, J. Hu, M. Curty, L. Qian, and H.-K. Lo, "Proof-of-principle experimental demonstration of twin-field type quantum key distribution," *Physical Review Letters*, vol. 123, no. 10, p. 100506, 2019.

[39] X.-T. Fang, P. Zeng, H. Liu, M. Zou, W. Wu, Y.-L. Tang, Y.-J. Sheng, Y. Xiang, W. Zhang, H. Li *et al.*, "Implementation of quantum key distribution surpassing the linear rate-transmittance bound," *Nature Photonics*, pp. 1–4, 2020.