Coincidence detection QKD protocol

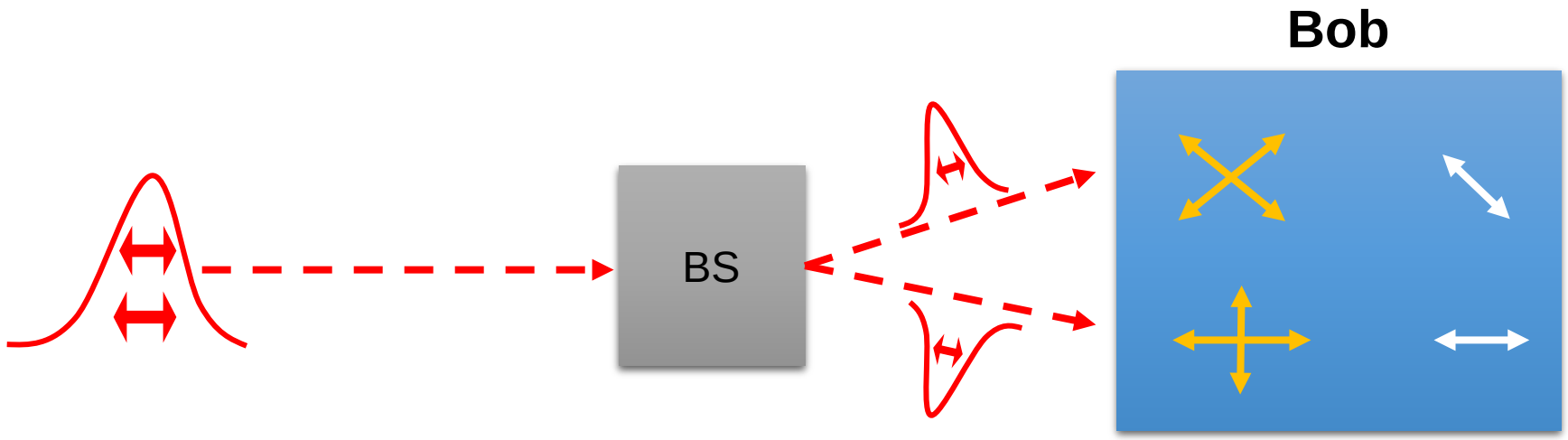
Ayan Biswas, Anindya Banerjee, Rupesh Kumar,
Pooja Chandravanshi, M.V. Jabir, Ali Anwar, Sarika Mishra,
G.K. Samanta, Shashi Prabhakar, R. P. Singh

Quantum Science & Technology Program
Atomic, Molecular and Optical Physics Division
Physical Research Laboratory (PRL), Ahmedabad

Quantum Technologies Laboratory
Photonic Sciences Laboratory
Attosecond Physics Laboratory
Crystal Defects and Luminescence Lab
Quantum Materials and Photonic Quantum Computing Lab
Atomic Physics: Theory

Coincidence Detection Protocol

- After protocol run Bob keeps the record of all the measurements including 2-fold and 3-fold coincidences.
- Sifting process is also similar to BB84 except for 2-fold and 3-fold Coincidences.
- Bob matches coincidences corresponding to Alice's bases and keep those results where at least one photon hits the correct basis.
- If the number of 2-fold and 3-fold coincidences fall below a threshold value they abort the protocol.

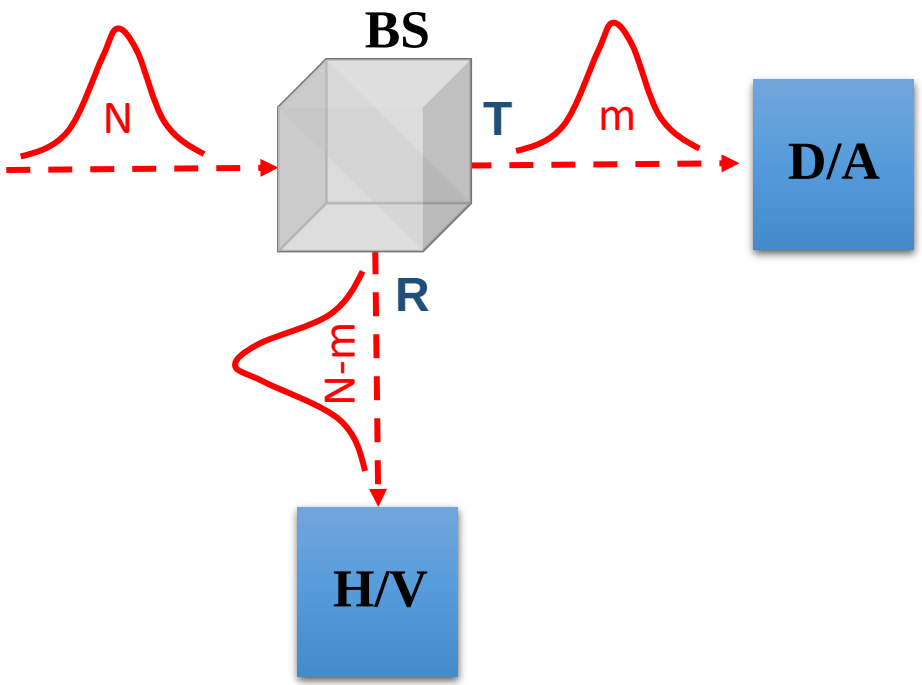


For 2 photon pulse incident on BS the cases are

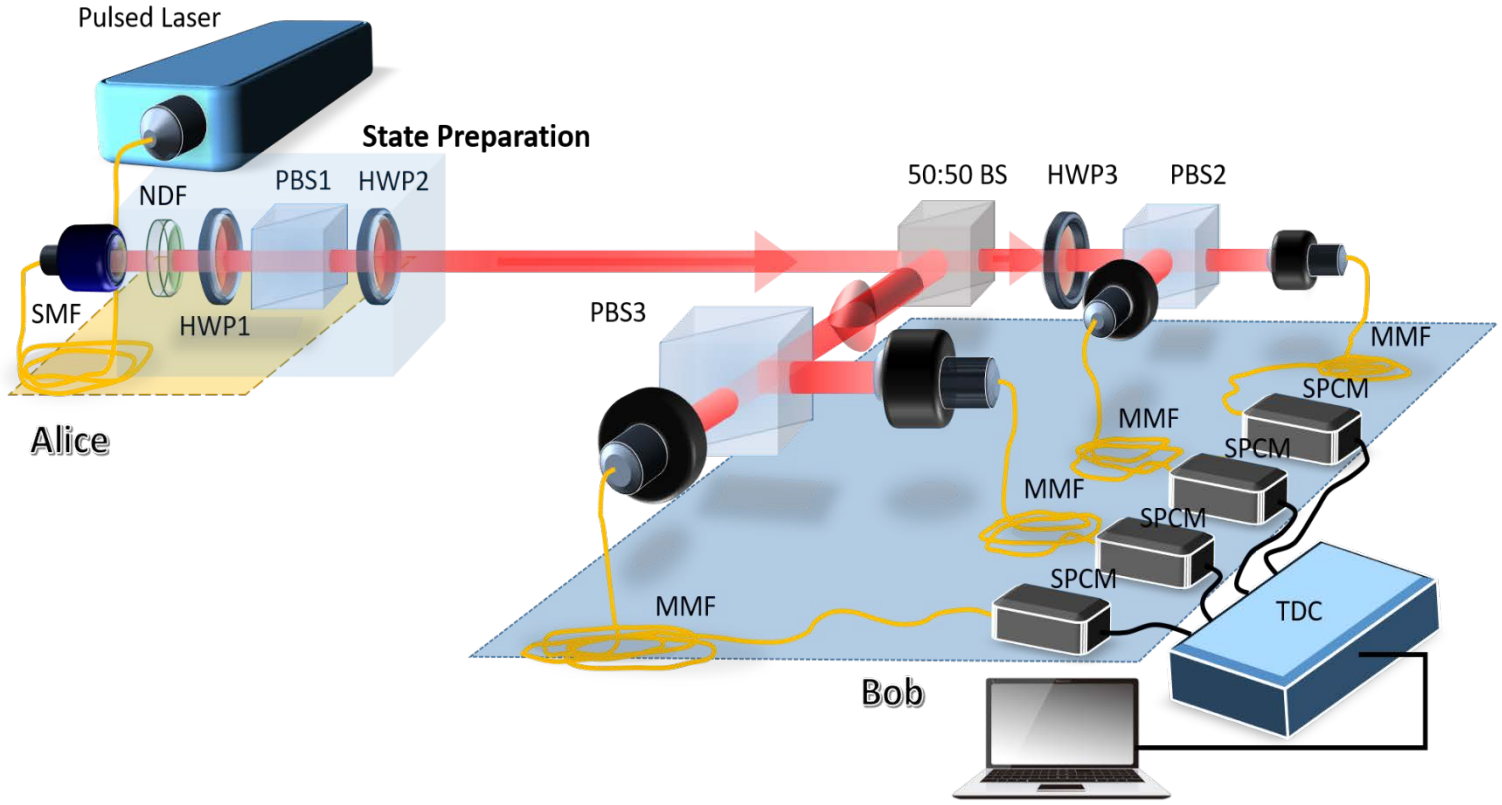
Possible Cases	(T)	(R)	Probability
1	2	0	1/4
2	0	2	1/4
3	1	1	1/2

For 3 photon pulse incident on BS the cases are

Possible Cases	(T)	(R)	Probability
1	3	0	1/8
2	0	3	1/8
3	2	1	3/8
4	1	2	3/8



Optical Setup for CD Protocol



Coincidences at Bob

$$N_C = \frac{1}{2} Y_2 p_2(\mu) + \frac{3}{4} Y_3 p_3(\mu)$$

Mean Photon Number (μ)	Total Coincidence (N_C)	
	Theoretical	Experimental
0.13	3178	3189±52
0.19	6414	6249±69
0.22	8828	8756±85
0.32	18657	18367±110
0.41	30337	30140±237

A. Biswas, A. Banerji, N. Lal, P. Chandravanshi, R. Kumar, and R. Singh, **Opt. Continuum** 1, 68-79 (2022), **doi: 10.1364/OPTCON.445727**

Key Rate for Coincidence Detection Protocol

$$R \geq \left\{ \frac{1}{2} Q_1 [1 - H_2(e_1)] + \frac{3}{4} Q_2 [1 - H_2(e_2)] + \frac{7}{8} Q_3 [1 - H_2(e_3)] - \frac{Q_\mu}{2} f(E_\mu) H_2(E_\mu) \right\}$$

Security Parameter $\Xi_{stat} = \Delta C_{stat} / C$ $\zeta = \frac{C}{S}$

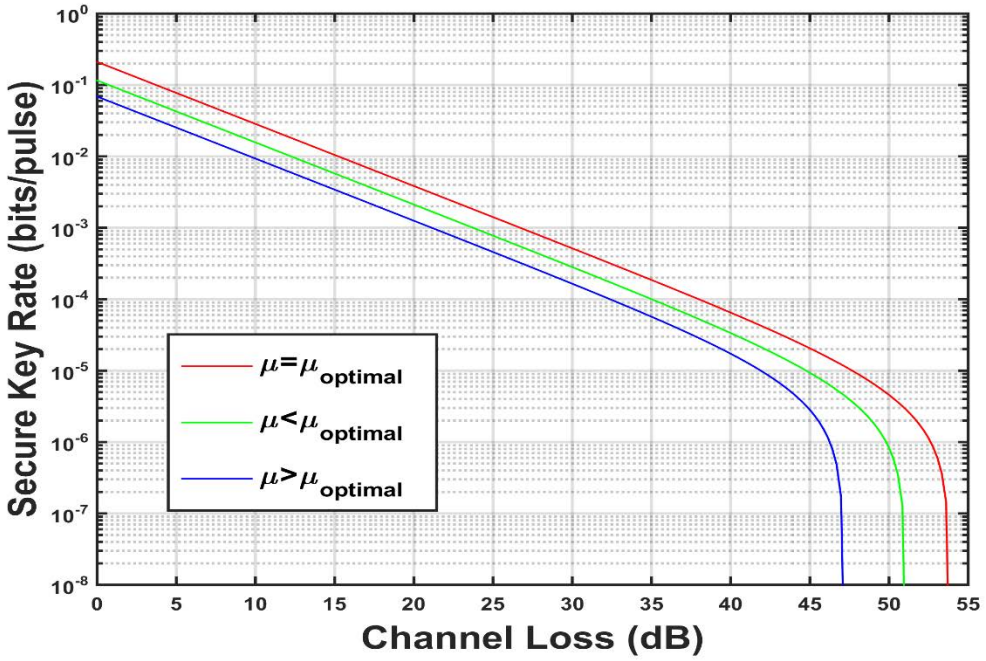


Figure: Key rate of CD protocol for various μ

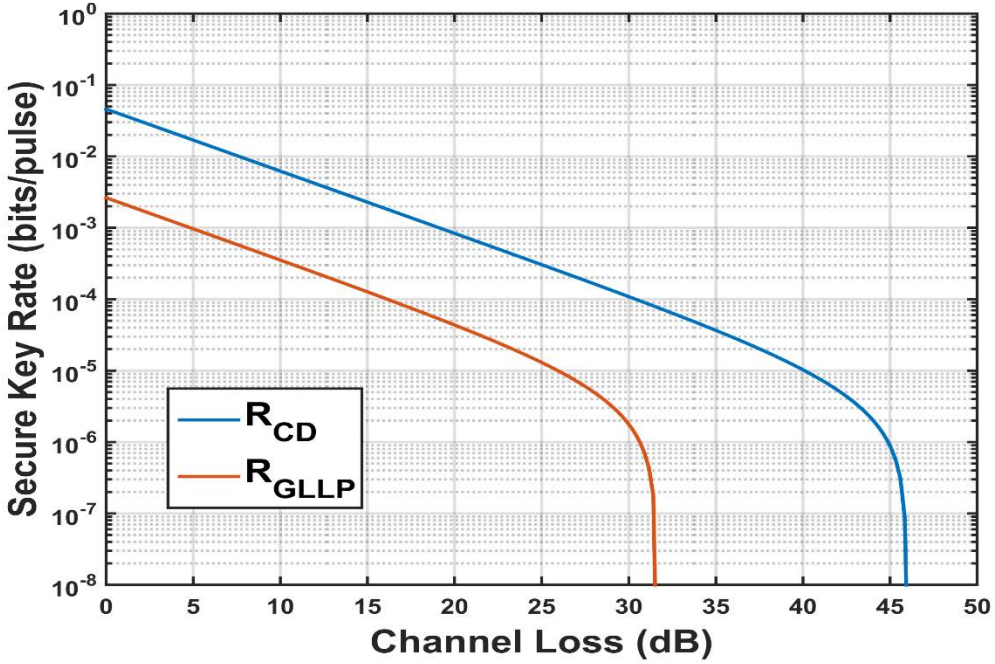


Figure: Comparison between GLLP protocol and CD Protocol

Security Parameters of CD Protocol

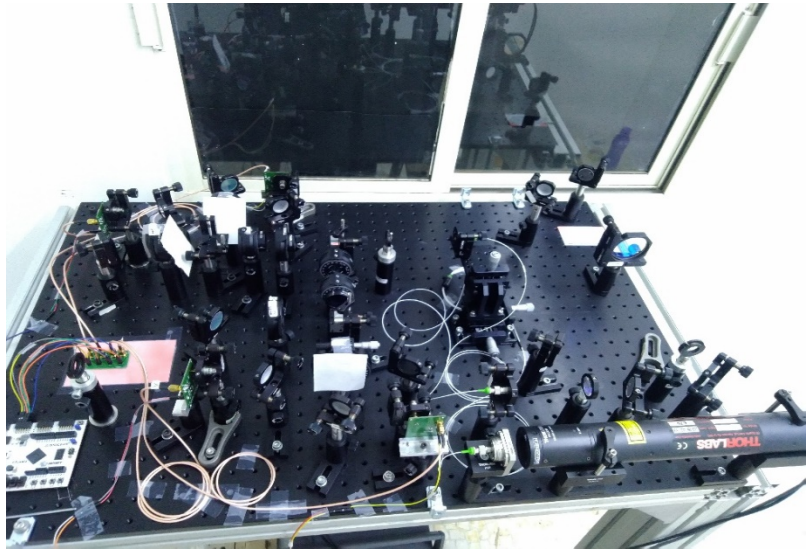
List of values for all the security parameters. C is the number of coincidences, ΔC_{stat} is the fluctuation in the number of the recorded coincidences, Ξ_{stat} is the ratio between ΔC_{stat} and C and ζ is the ratio between C and the number of detected singles. The numbers in brackets for each of the parameters are from the theoretical modelling of the protocol for a given channel attenuation. The values of α and β are taken to be 0.01 corresponding to a 1 % variation in the values of μ and η respectively.

Parameters	*Values*				
μ	0.13	0.19	0.22	0.32	0.41
C	3178 (3189)	6249 (6414)	8756 (8828)	18367 (18657)	30140 (30337)
ΔC_{stat}	53 (64)	69 (140)	85 (200)	111 (250)	237 (340)
Ξ_{stat}	0.016 (0.020)	0.011 (0.012)	0.0097 (0.023)	0.0065 (0.014)	0.0079 (0.11)
ζ	0.042 (0.066)	0.059 (0.098)	0.069 (0.115)	0.102 (0.169)	0.128 (0.218)

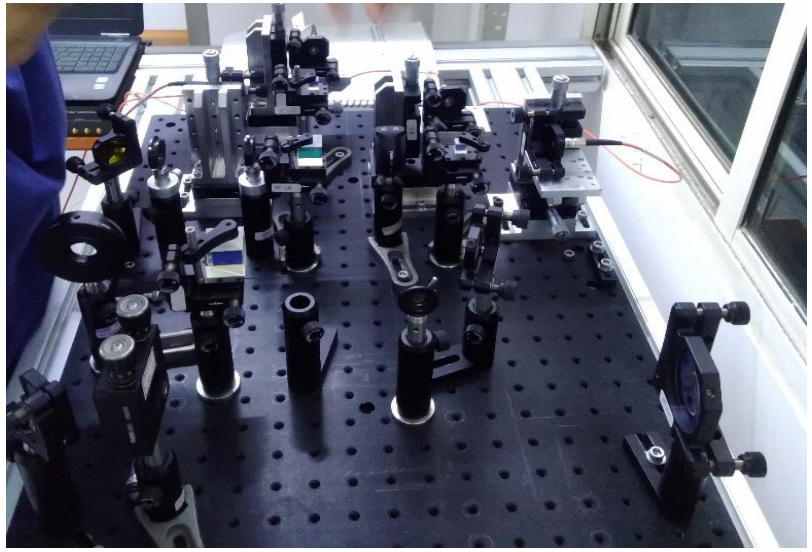
A. Biswas, A. Banerji, N. Lal, P. Chandravanshi, R. Kumar, and R. Singh, **Opt. Continuum** 1, 68-79 (2022), **doi: 10.1364/OPTCON.445727**

Demonstration of BB84 and BBM92 Protocol over 200 meters

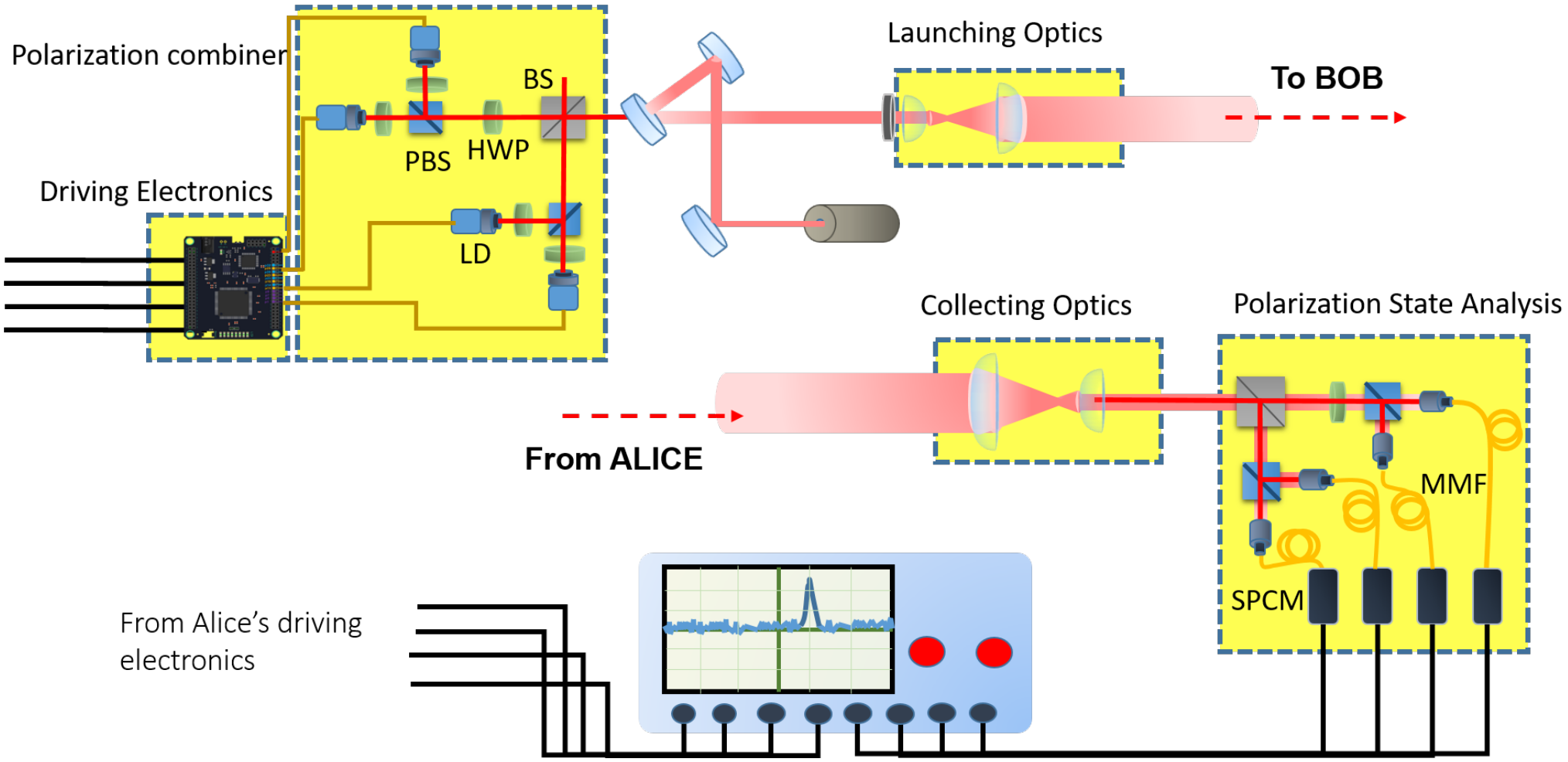
Transmitter (Alice)



Receiver (Bob)



Optical Setup for BB84 Protocol



BB84 Protocol over 200 meters

Parameter Estimation

Channel Transmissivity (η_{Ch})=**0.70**
Mean Photon Number (μ)=**0.3**

Overall Detector Efficiency(η_{det})=**0.4**
Repetition Rate of Laser (f_{rep})=**5 MHz**

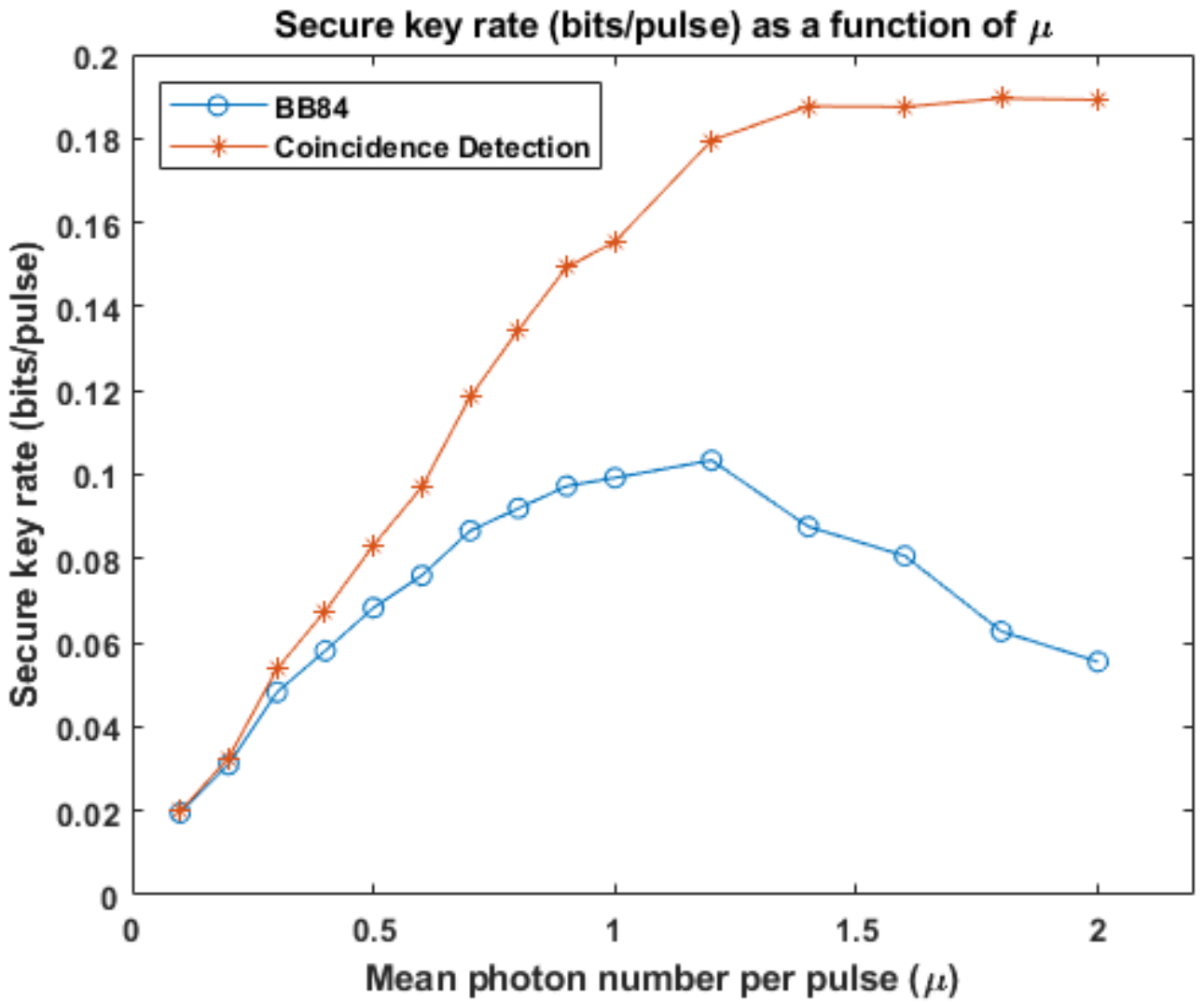
TABLE: *Showing QBER and Key Rate for some sets taken at random from detections*

Set No	Transmitted (R_T)	Detections (R_D)	Sift key (R_{Sif})	Error Bits (E_B)	QBER (%) $\left(E_B/R_{Sif}\right)$
1	50462	4435	2154	62	2.8
2	50518	4010	1936	65	3.3
3	50546	1940	1894	44	2.2

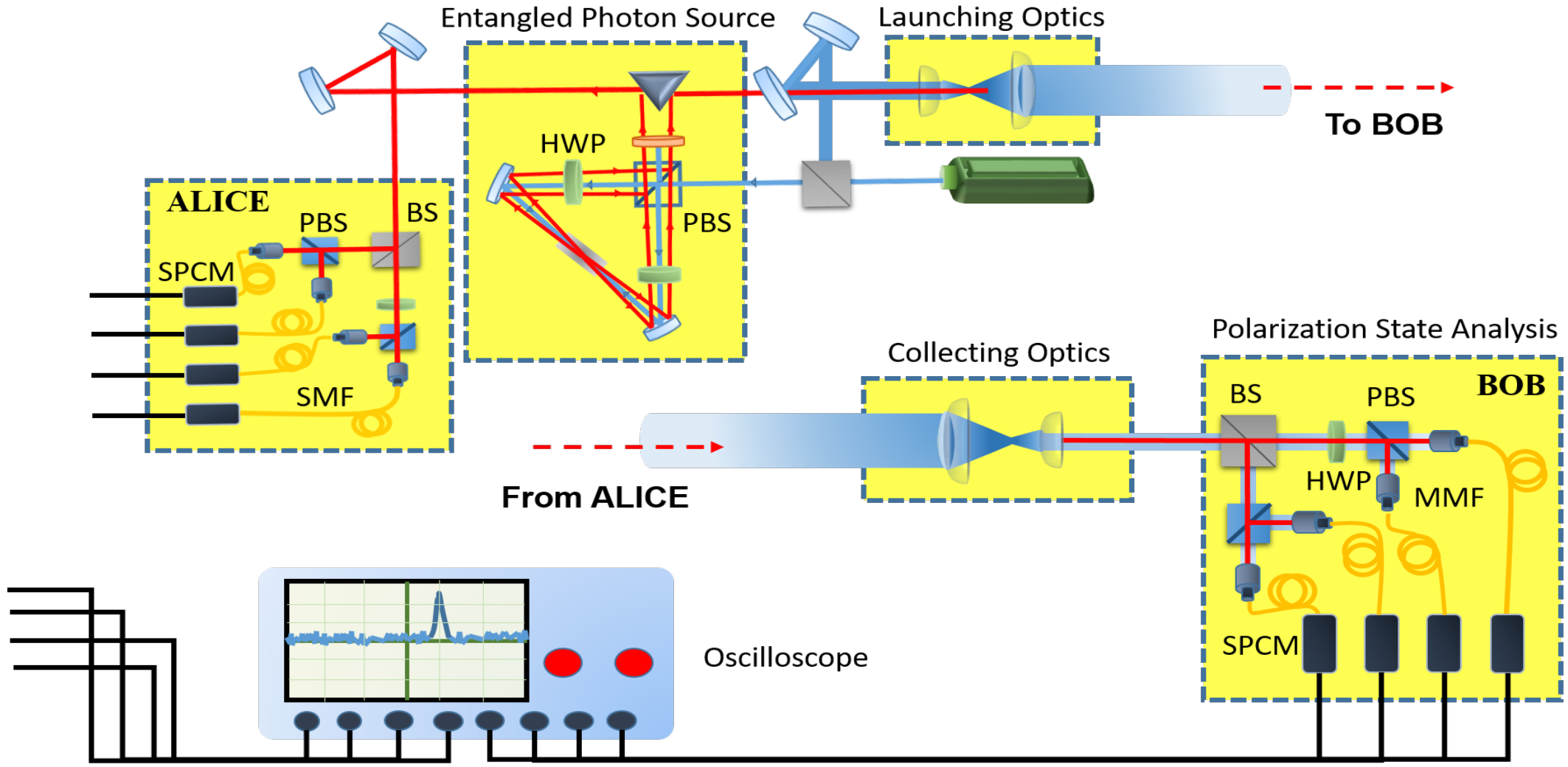
Average Sift Key Rate (K) **~ 200 Kbps**

Secret Key Rate (K_s) **~ 140 Kbps**

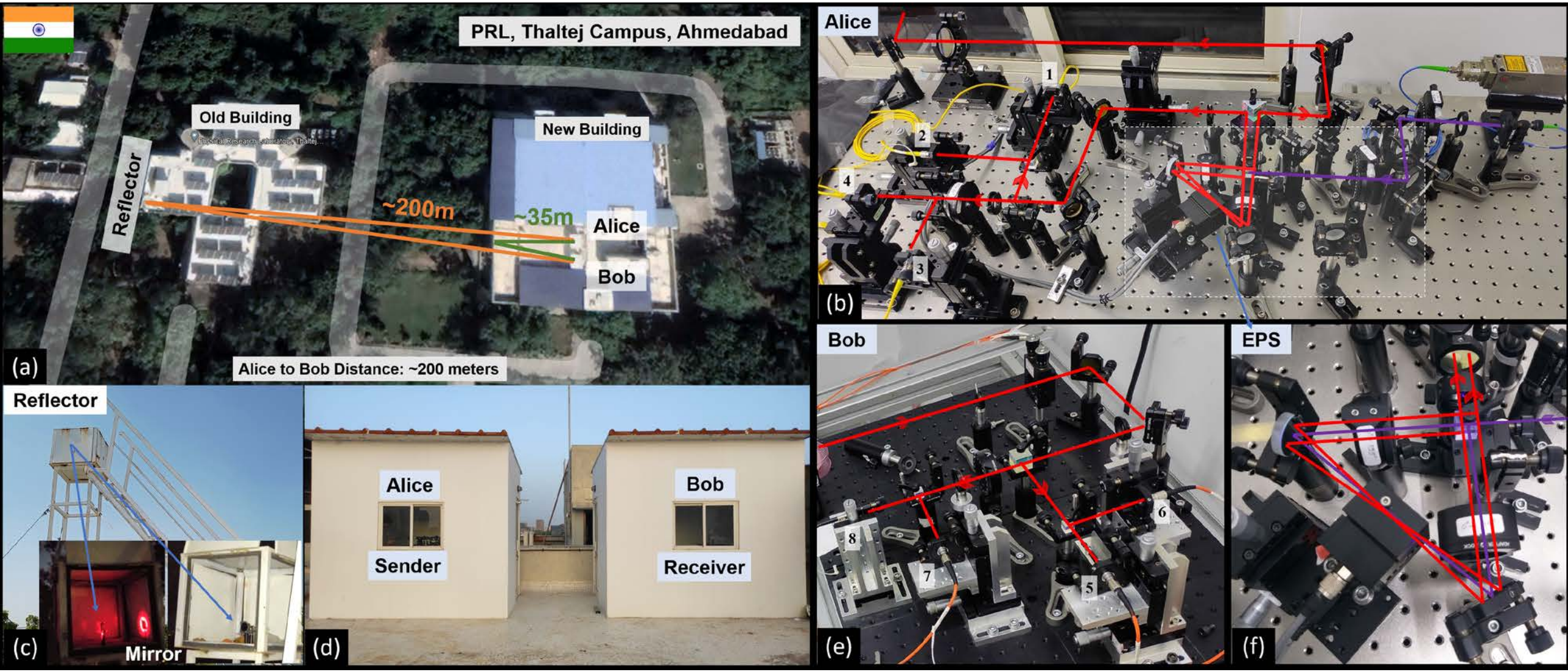
Results for 200 atmospheric channel



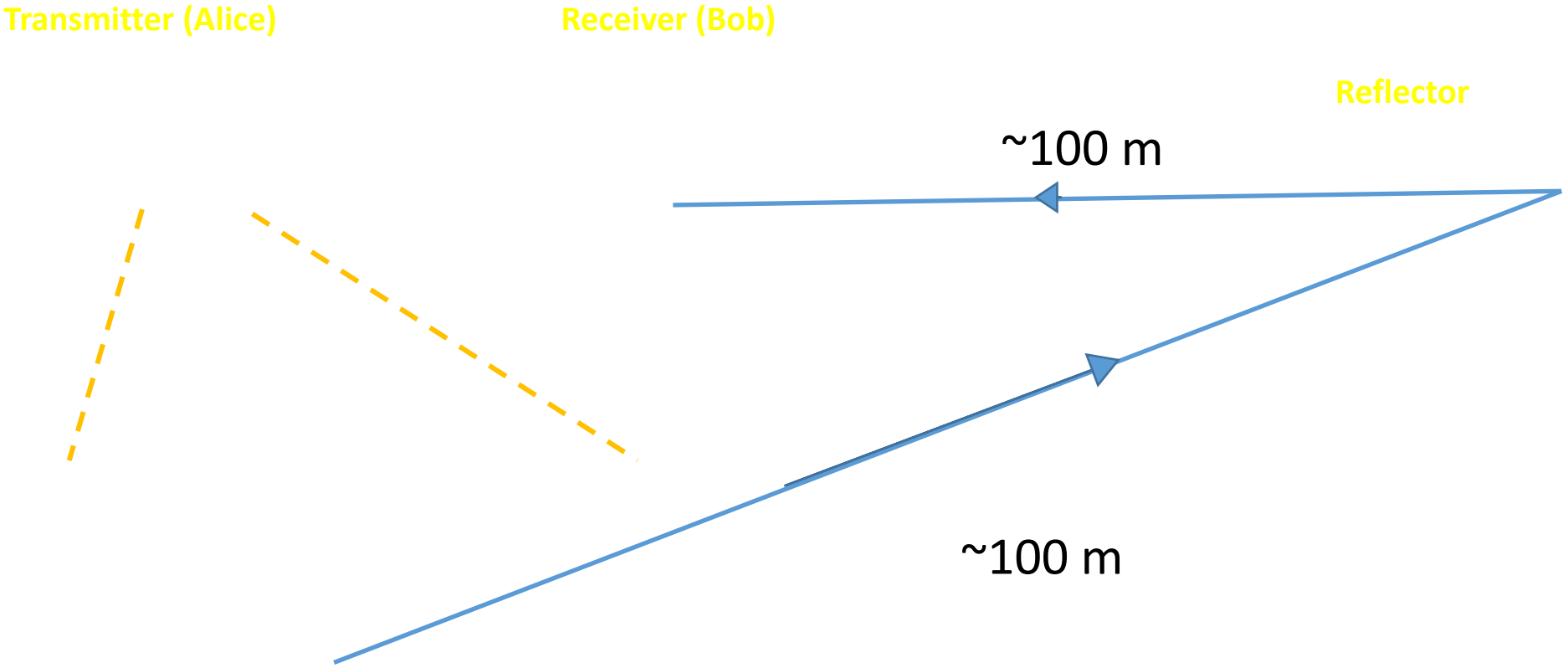
Optical Setup for BBM92 Protocol



S. Mishra, A. Biswas, S. Patil, P. Chandravanshi, V. Mongia, T. Sharma, A. Rani, S. Prabhakar, S. Ramachandran, R. P. Singh, **24 (2022) 074002.**

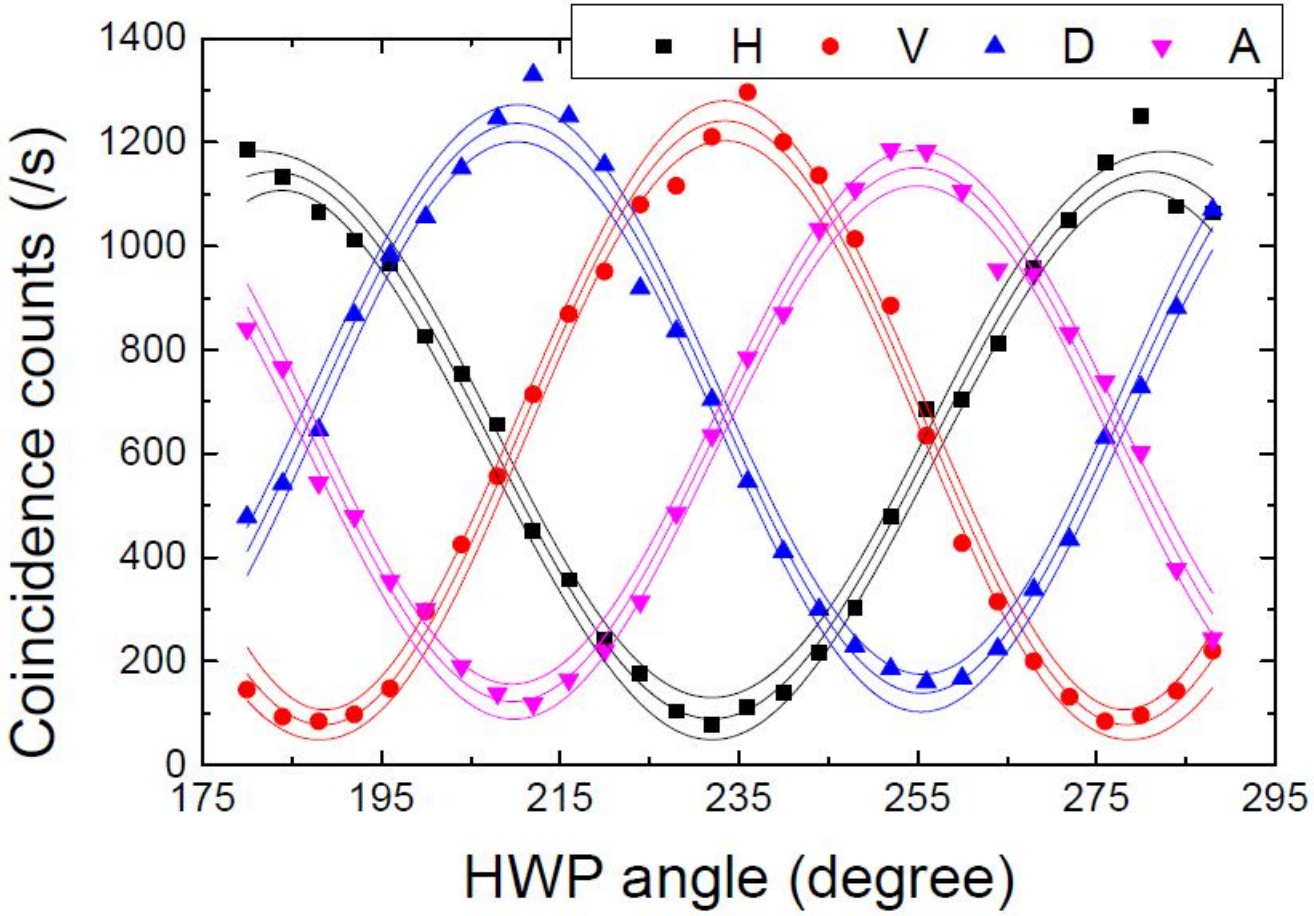

PRL, Thaltej Campus, Ahmedabad
Old Building
New Building
Reflector
~200m
~35m
Alice
Bob
(a)
Alice to Bob Distance: ~200 meters
Alice
1
2
3
4
(b)
Reflector
Mirror
(c)
Alice
Sender
Bob
Receiver
(d)
Bob
5
6
7
8
(e)
EPS
(f)

Free space BB84 Protocol in the field



Entanglement Distribution over 200 meters

Correlation of polarization states between Alice and Bob



Coincidence window = 1 ns

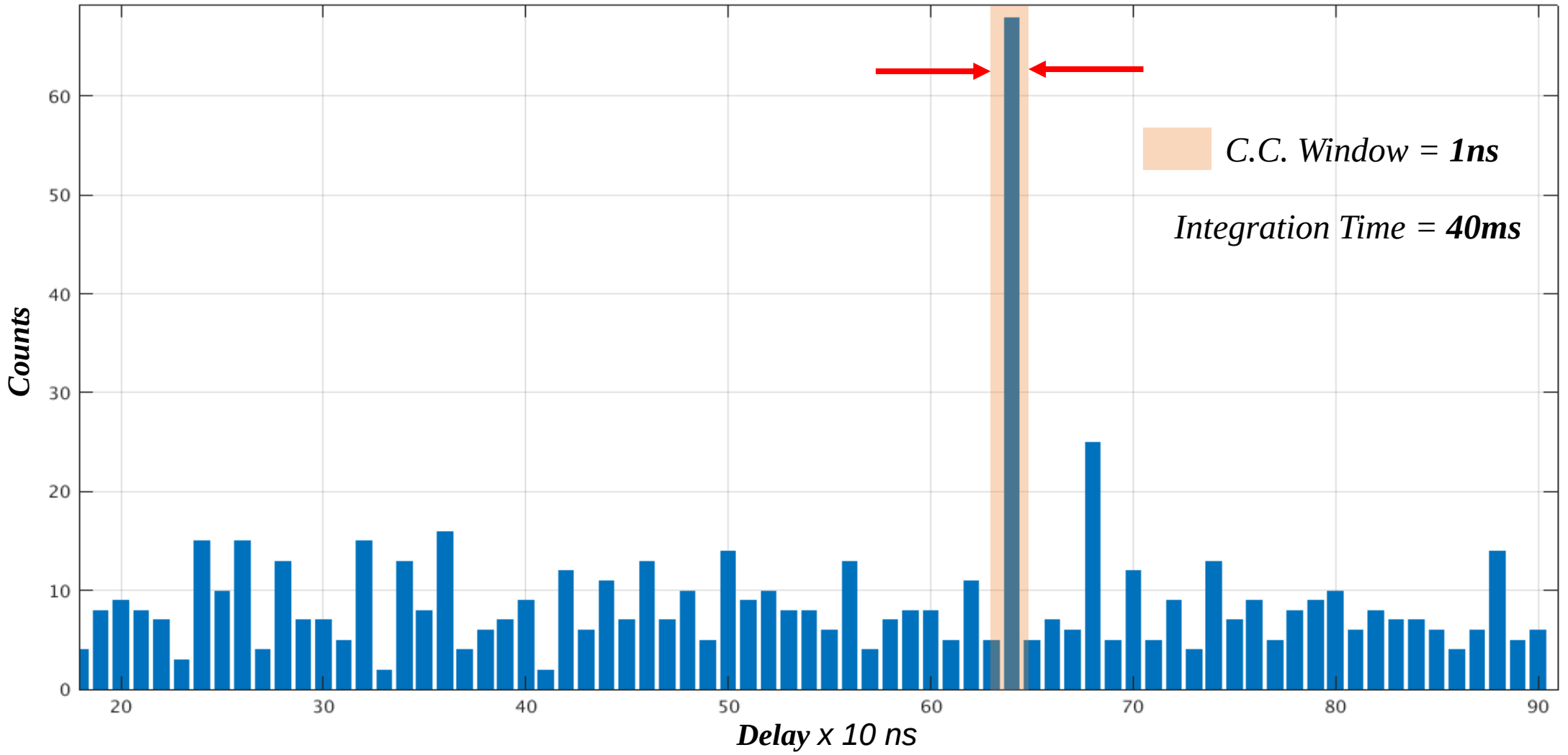
Bell's Parameter

S=2.54

Polarization Visibility

H	V	D	A
94.2%	93.66%	83.33%	87.53%

Temporal Filtering



*Delay from Alice's **H** pol. state detector to Bob's **H** pol. State detector = **648ns***

BBM92 Protocol over 200 meters

Parameter Estimation

Channel Transmissivity (η_{Ch})=**0.70** Overall Detector Efficiency(η_{det})=**0.4** Background Coincidences=**40**

TABLE: *Showing QBER and Key Rate for BBM92 Protocol*

ALICE \ BOB	H	V	D	A
H	1023	41	603	501
V	36	1167	661	592
D	408	671	1287	76
A	644	591	117	1140

Average Sift Key Rate (K) ***= Total CC in correct basis detectors*** **= 4.5 kbps**

QBER= CC in wrong detectors/total CC= **4%**

Secure key rate **~ 1.7 kbps**

Atmospheric conditions, mean and variance from midnight to 6 AM (typical measurement time for our experiments)

Date	Extinction (Mm-1)	Scattering (Mm-1)	PM2.5 (µg/m3)
08/05/2021	76.41±7.78	62.73±5.82	2.87±0.26
10/05/2021	48.67±6.70	40.16±6.15	1.68±0.24

Parameters	35 m	200 m
Channel transmission (%)	94	70
CHSH Bell parameter (S)	2.51±0.06	2.54±0.06
Mean visibility (%)	88.85±5.39	90.99±5.89
QBER (%)	5.58	4.50
Sifted key rate (kbps)	6.37	4.89
Key rate after EC (kbps)	6.01	4.20
Key rate after PA (kbps)	2.33	1.71
Secure key rate (kbps)	2.33	1.71

Summary

- Proposed a new protocol to increase the secure key rate using the same resources as in BB84 protocol.
- Demonstrated the feasibility of CD protocol for atmospheric channel of 200 meters.

Future plan of work at QST Program @ PRL

- Effect of turbulence and how to mitigate it for terrestrial communication.
- Simulating conditions for uplink and downlink to check the key rate for satellite based quantum communication.
- Development of Device Independent QKD protocol.
- Entanglement swapping and quantum teleportation in free space for 200 meters towards setting QC network
- Using structured light such as - Vortex beam, Pencil beam, Gaussian Schell Model beam, Twisted Gaussian Schell Model beam - for robust and secure key distribution
- **Development of Photonic Quantum Computing since it is the best bet for quantum internet, the ultimate stage of quantum communication (China, Xanadu in Canada and Psi Quantum in USA, ORCA Computing in UK are making good progress)**

Thank you