Plug-and-play differential phase encoded measurement-device-independent QKD protocol

Shashank Kumar Ranu[1,2], **Anil Prabhakar**[1], **Prabha Mandayam**[2]

[1]*Department of Electrical Engineering, Indian Institute of Technology, Chennai-600036, India*
[2]*Department of Physics, Indian Institute of Technology, Chennai-600036, India*

ee16s300@ee.iitm.ac.in, anilpr@ee.iitm.ac.in, prabhamd@physics.iitm.ac.in

Active stabilization systems are typically used in MDI implementations to ensure indistinguishability of photons from Alice and Bob, mainly in three dimensions: spectrum, polarization, and timing [1,2]. These stabilization systems increase the complexity of QKD experiments. Plug-and-play architecture reduces the experimental complexity arising because of reference frame alignment between Alice and Bob [3,4].

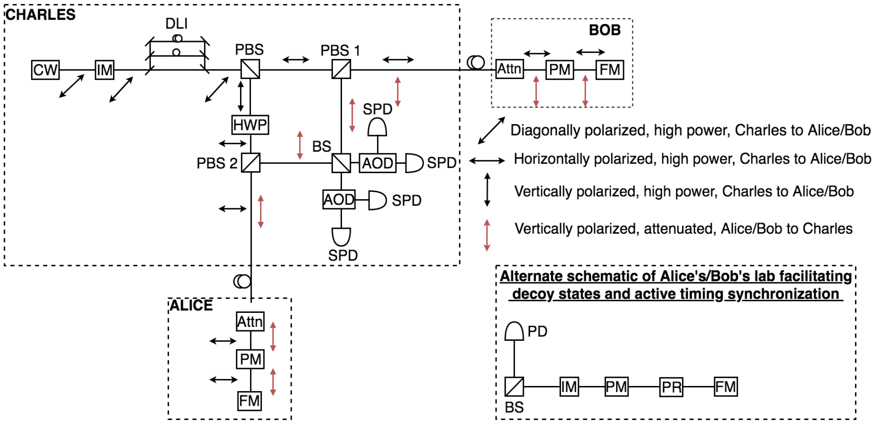
CHARLES
DLI
CW
IM
PBS
PBS 1
HWP
PBS 2
BS
SPD
AOD
SPD
AOD
SPD
SPD
BOB
Attn
PM
FM
ALICE
Attn
PM
FM
Diagonally polarized, high power, Charles to Alice/Bob
Horizontally polarized, high power, Charles to Alice/Bob
Vertically polarized, high power, Charles to Alice/Bob
Vertically polarized, attenuated, Alice/Bob to Charles
Alternate schematic of Alice's/Bob's lab facilitating decoy states and active timing synchronization
PD
BS
IM
PM
PR
FM

Fig. 1. Schematic of plug-and-play DPS MDI. CW = Continuous Wave laser, PC = Polarization controller, DLI = Delay Line Interferometer, PBS = Polarization Beamsplitter, HWP = Half-Wave Plate, BS = Beamsplitter, AOD = Acousto-Optic Deflector, SPD = Single-Photon Detector, IM = Intensity Modulator, PM = Phase Modulator, PR = Phase randomizer, FM = Faraday Mirror.

We have previously proposed a differential phase-encoded MDI protocol (DPS MDI), and using a decoy state analysis, we estimated the length of a secure channel for a weak coherent source (WCS) based implementation [5]. We use the WCS DPS MDI protocol for designing a plug-and-play DPS MDI scheme (see Fig. 1). In $n = 3$ DPS MDI, Alice and Bob encode their key information as phase difference between two time-bins. As these time bins are few nanoseconds apart, the quantum channel affects them in a similar way, thereby cancelling the effects of phase fluctuations. In other MDI protocols that use pulse-train, such as B92 MDI, Alice and Bob encode key information as phase of an individual pulse [6]. This applied phase gets affected by random fluctuations and results in higher QBER [7]. Note that, $n > 3$ DPS MDI would lead to increased complexity in key reconciliation scheme as well as in its implementation [8].

As Alice and Bob use independent lasers, an optical phase-locked loop (OPLL) is required to share a phase reference in MDI implementations. Using a single laser in our plug-and-play architecture removes the requirement of an OPLL. Further, Alice and Bob use independent delay lines to create three time-bins in DPS-MDI. The time-bins of Alice and Bob differ due to variations in their respective DLIs. Use of a single DLI in the plug-and-play scheme solves this issue. Hence, our plug-and-play differential phase encoding offers protection against random phase fluctuations along with ease of implementation.

References

1. T Ferreira Da Silva, D Vitoreti, GB Xavier, GC Do Amaral, GP Temporao, and JP Von Der Weid. Proof-of-principle demonstration of measurement-device-independent quantum key distribution using polarization qubits. *Physical Review A*, 88(5):052303, 2013.
2. Zhiyuan Tang, Zhongfa Liao, Feihu Xu, Bing Qi, Li Qian, and Hoi-Kwong Lo. Experimental demonstration of polarization encoding measurement-device-independent quantum key distribution. *Physical Review Letters*, 112(19):190503, 2014.
3. A Muller, T Herzog, B Huttner, W Tittel, H Zbinden, and N Gisin. plug and play systems for quantum cryptography. *Applied Physics Letters*, 70(7):793–795, 1997.
4. Yujun Choi, Osung Kwon, Minki Woo, Kyunghwan Oh, Sang-Wook Han, Yong-Su Kim, and Sung Moon. Plug-and-play measurement-device-independent quantum key distribution. *Physical Review A*, 93(3):032319, 2016.
5. Shashank Kumar Ranu, Anil Prabhakar, and Prabha Mandayam. Differential phase encoded measurement-device-independent quantum key distribution. *arXiv preprint arXiv:1905.11153*, 2019.
6. Agnes Ferenczi. *Security proof methods for quantum key distribution protocols (PhD thesis)*. University of Waterloo, 2013.
7. Xiongfeng Ma, Pei Zeng, and Hongyi Zhou. Phase-matching quantum key distribution. *Physical Review X*, 8:031043, Aug 2018.
8. Gautam Shaw, Shyam Sridharan, Shashank Ranu, Foram Shingala, Prabha Mandayam, and Anil Prabhakar. Equivalence of space and time-bins in DPS-QKD, 2020.