Plug and Play Measurement Device Independent quantum secure communication

Anuj Sethia[1], Jordan Smith[1], Hanen Chenini[1], Ashutosh Singh[1], Amir Ahadi[1,2], Nick Kuzmin[1], and Daniel Oblak[1]

[1]Department of Physics and Astronomy & Institute of Quantum Science and Technology, University of Calgary, Calgary, AB, T2N 1N4, Canada

[2]Department of Electrical and Computer Engineering, University of Calgary, Calgary, AB, T2N 1N4, Canada

2023 IEEE Photonics Conference (IPC) | 979-8-3503-4722-7/23/$31.00 ©2023 IEEE | DOI: 10.1109/IPC57732.2023.10360772

***Abstract*—We experimentally demonstrate a commercially viable plug and play Measurement Device Independent Quantum Key Distribution (MDI-QKD) prototype. MDI-QKD allows for sharing of critical components such as single photon detectors by multiple users, making it an ideal choice for star-type topology quantum networking.**

***Index Terms*—quantum communication, quantum key distribution**

I. Introduction

The advent of quantum computers will enable solving some complex mathematical problems in a feasible time scale compared to classical computers [1]. Unfortunately, classical cryptography is contingent upon the difficulty of mathematical problems such as prime factorisation of large numbers. Quantum computers could solve such problems in polynomial time, and thus would render conventional cryptography obsolete. Fortunately, Quantum Key Distribution (QKD) is an ingenious technology for information-theoretic secure communication between two distant parties and, hence, is unaffected by any advances in computational capabilities. However, a practical QKD system faces numerous challenges in hardware development, communication distance, security robustness, and cost [2]. Moreover, the realistic implementation of some QKD protocols are insecure due to device imperfections and hardware limitations [3]. MDI-QKD is an innovative protocol proven to be secure against all detector side-channel attacks by an eavesdropper [4]. In this work, we showcase a commercially viable MDI-QKD prototype for effortless deployment to existing telecommunication networks.

II. Protocol

The MDI-QKD protocol [4] mainly involves three parties: the two end users (Alice and Bob) and a central untrusted node Charlie. Charlie is the central detection hub which allows cost-effective key distribution among multiple users in a star-type topology. In our implementation, we employ time-bin qubits for MDI-QKD for encoding information and seamless adaptation to the existing telecommunications networks.

The protocol can be described as follows. Firstly, the end users prepare weak coherent pulses for time-bin qubits in the states mentioned below. The intensity of the states is also varied randomly to produce signal and decoy states in order to avoid photon number splitting attack due to weak coherent states. The state are prepared randomly and independently using only off-the-shelf optical components by both Alice and Bob. These photonic qubits are sent to Charlie via an optical fibre link for partial Bell State Measurements (BSM) by interfering them on a 50:50 beam splitter. Charlie announces the projection onto $|\psi^-\rangle = \frac{1}{\sqrt{2}}(|e_{D1}l_{D2}\rangle - |l_{D1}e_{D2}\rangle)$ detection. The users perform basis reconciliation over an authenticated public channel by discarding qubit pairs prepared in different bases. Additionally, either of the user performs a bit-flip to correct anti-correlations from $|\psi^-\rangle$ projection. Finally, error-correction and privacy amplification is performed to obtain final secure encryption key.

Bit	Z-basis	X-basis
1	$\|e\rangle$	$\frac{1}{\sqrt{2}}(\|e\rangle + \|l\rangle)$
0	$\|l\rangle$	$\frac{1}{\sqrt{2}}(\|e\rangle - \|l\rangle)$

III. Experiment

Our experimental setup for MDI-QKD prototype is shown in figure 1. As mentioned, the end users prepare time-bin qubits using telecommunication components such as lasers diodes (LD), intensity modulator (IM) and phase modulator (PM). The LD prepare phase randomised optical pulses every clock cycle with a period of 5 ns. The time-bin qubits of 200 ps are carved out from the laser pulses using the first IM in the schematic and the PM applies π phase shift only for $|-\rangle$ state. The second IM modulates the intensity of overall time-bins corresponding to signal, decoy and vacuum states. An Field Programmable Gate Arrays (FPGA) along with auxiliary electronics prepare both RF and DC signals for randomised state generation. Finally, a Variable Optical Attenuator (VOA) reduces the intensity of each pulses to single photon level and the isolator (ISO) protects back reflections from an eavesdropper.

At the central node, Charlie aligns for polarisation of qubits from users using Polarisation Controller (PC) and Polarisation Beam Splitter (PBS). Lastly, the two qubits are interfered on a 50:50 beam splitter for BSM and resulting photons are detected using Superconducting Nanowire Single Photon Detectors (SNSPDs) in a cryostat. The detection of photons

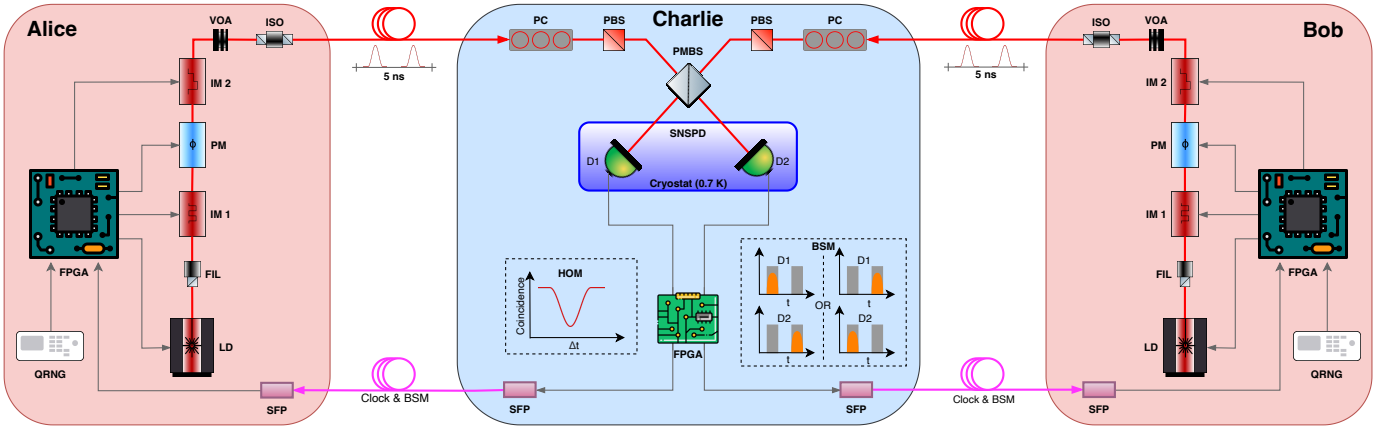

Fig. 1. Schematic of time-bin qubit based MDI-QKD prototype.

by both the detectors in alternative time-bins corresponds to projection onto $|\psi^-\rangle$ state. The FPGA recognises the detection patterns and communicates the results to the end users for key reconciliation.

The most critical as well as challenging requirement for MDI-QKD is to maintain indistinguishability of photon from different users for the quantum interference. The photons arriving from the users must be identical in terms of timing, polarisation, spatial mode and frequency degree of freedom. Any deviation from this condition would reduce the Hong-Ou-Mandel (HOM) interference visibility, resulting in errors. The HOM visibility is usually measured by observing coincidence clicks on two detectors to keep track of the photon indistinguishability. Active feedback mechanisms are required for all degrees of freedom to ensure efficient real world deployment. For instance, the PCs at Charlie needs to be actively adjusted to ensure maximum photon from the selected PBS port.

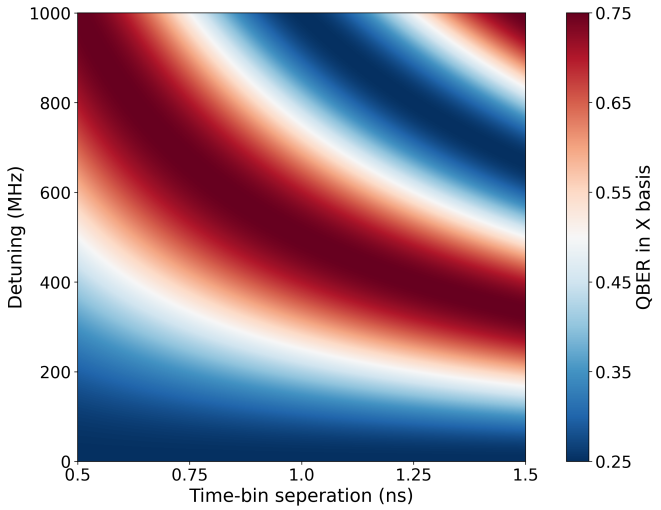

Fig. 2. Error in X-basis dependence on laser detuning and time-bin separation

The frequency stabilisation of Alice's and Bob's laser is undoubtedly the most demanding challenge for MDI-QKD as frequency difference between the two users would result in phase errors, leading to higher QBER for X-basis events. The figure 2 shows the sensitivity of laser frequency detuning for different time-bin separation on the X-basis QBER. Interestingly, the minimum QBER in X-basis is limited to 25% because of multi-photon instance in the weak coherent pulses. For a 1 ns time-bin separation the lasers at Alice and Bob needs to be locked within 25 MHz to limit the QBER to 26%. Several approaches have been explored for locking the lasers of each user. One approach is to monitor the optical beat signal however, the users need to send CW light to Charlie, requiring additional fibre links. Interestingly, Tang et al. demonstrated using HOM interference visibility at the expense of interrupting qubit exchange [5]. In this work, we showcased an interruption free laser locking feedback mechanism for the challenging requirements of MDI-QKD.

References

[1] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM J. Comput.*, vol. 26, p. 1484–1509, oct 1997.

[2] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, "Secure quantum key distribution with realistic devices," *Rev. Mod. Phys.*, vol. 92, p. 025002, May 2020.

[3] S. Sun and A. Huang, "A review of security evaluation of practical quantum key distribution system," *Entropy*, vol. 24, no. 2, 2022.

[4] H.-K. Lo, M. Curty, and B. Qi, "Measurement-device-independent quantum key distribution," *Phys. Rev. Lett.*, vol. 108, p. 130503, Mar 2012.

[5] Y.-L. Tang, H.-L. Yin, Q. Zhao, H. Liu, X.-X. Sun, M.-Q. Huang, W.-J. Zhang, S.-J. Chen, L. Zhang, L.-X. You, Z. Wang, Y. Liu, C.-Y. Lu, X. Jiang, X. Ma, Q. Zhang, T.-Y. Chen, and J.-W. Pan, "Measurement-device-independent quantum key distribution over untrustful metropolitan network," *Phys. Rev. X*, vol. 6, p. 011024, Mar 2016.