Resource-efficient real-time polarization compensation for MDI-QKD with rejected data

Olinka Bedroya\textsuperscript{1†}, Chenyang Li\textsuperscript{2}, Li Qian\textsuperscript{2}, and Hoi-Kwong Lo\textsuperscript{1,2,3}

\textsuperscript{1}Centre for Quantum Information and Quantum Control, Dept. of Physics, University of Toronto, Toronto, Ontario, M5S 1A7, Canada
\textsuperscript{2}Centre for Quantum Information and Quantum Control, Dept. of Electrical & Computer Engineering, University of Toronto, Toronto, Ontario, M5S 3G4, Canada
\textsuperscript{3}Department of Physics, University of Hong Kong, Pokfulam, Hong Kong
\textsuperscript{†}o.bedroya@mail.utoronto.ca

Abstract: We propose and implement a novel polarization compensation in MDI-QKD systems using discarded bits, without reducing key-sharing cycle or demanding additional resources. Polarization drift is maintained below 0.15 rad over 40 km of fibre. © 2021 The Author(s)

Quantum key distribution (QKD) allows two parties to share a secret key over an insecure channel and is proven to be information-theoretically secure. However, the devices used in practice deviate from the perfect models used in security proofs, and this deviation compromises security. Measurement-device-independent quantum key distribution (MDI-QKD)\textsuperscript{[1]} closes all possible side channels on the detection system, such that measurement can be done by an untrusted third party who performs a Bell state measurement on the states received from two users.

Bell state measurement requires polarization alignment. However, due to the fibre’s temperature fluctuations and birefringence, maintaining the polarization in long fibres is challenging (figure 1(a)). Maintaining the polarization is even more complicated for polarization-encoding MDI-QKD compared to time-bin or phase encodings. This is because, in polarization encoding MDI-QKD, Bell state measurement’s indistinguishability condition requires perfect alignment of both bases (rectilinear and diagonal) of two users rather than one.

In available QKD literature, compensation always comes at a cost. The drawbacks fall into one of the three categories: (1) the key sharing needs to be interrupted \textsuperscript{[2]}, (2) some additional resource is required to multiplex reference polarization pulses with the signal \textsuperscript{[3]}, (3) a fraction of quantum pulses are sacrificed for tomography \textsuperscript{[4]}\textsuperscript{[1]}. We propose and implement a polarization compensation scheme that avoids all of those drawbacks using some of the MDI-QKD’s discarded detections.

Our novel polarization compensation scheme solely relies on rejected data. In MDI-QKD, only coincident detections corresponding to successful Bell state measurements are used for key generation (table 1(a)), and all the single events are discarded. Additionally, detection events associated with decoy states do not contribute to the key sharing. In decoy-state QKD, the vacuum state is usually used as one of the decoy states as it allows the users to estimate the background rate. When one user is sending a vacuum decoy-state, the detection result provides direct information about the polarization state prepared and sent by the other user (table 1(b)). We use the single detection measurements corresponding to these transmitted states to actively evaluate the polarization drift based on singles’ error rates and run compensation independently for each user. As it can be seen in table 1, detections due to 25.5% of transmitted states which were previously discarded, could be recycled and used. To put this number in perspective, only 10.1% of transmitted states could contribute to the secret key (table 1(a)).

We verified the feasibility of real-time compensation over a 40 km distance. The fibre spools were left exposed and without isolation. The actuation solely relies on polarization controllers within the measurement setup and in the channel (either at the outputs of users or inputs of measurement node), which are required for MDI-QKD regardless of the implementation. The polarization controllers in the channels are used to independently maintain each user’s alignment to the measurement node by minimizing the aforementioned single counts’ error rates. Figure 1(b) shows the polarization misalignment in two bases for two users over three hours (estimated from the error-rates using $\sin^{-1}$). The compensation scheme can successfully maintain the singles’ error rate below 2.25% (corresponding to a misalignment below 0.15 rad) for each basis and each user. The overall QBER (from Bell state measurements coincidences) is below 3%. The decoy intensities used in our experiment are optimized based on\textsuperscript{[6]} to be $\mu = 0.28$, $\nu = 0.07$ and $\omega = 0.001$ photon per pulse, with corresponding probabilities $P_\mu = 0.52$, $P_\nu = 0.33$ and $P_\omega = 0.15$.

\textsuperscript{1}We are aware of only one exception to this classification \textsuperscript{[5]}. However, this scheme does not apply to MDI-QKD.
Alice Bob Probability
\(|H_\mu\rangle\) \(|V_\mu\rangle\) 1.7%
\(|V_\mu\rangle\) \(|H_\mu\rangle\) 1.7%
\(|+\mu\rangle\) \(|+\mu\rangle\) 1.7%
\(|-\mu\rangle\) \(|-\mu\rangle\) 1.7%
\(|+\mu\rangle\) \(|-\mu\rangle\) 1.7%
\(|-\mu\rangle\) \(|+\mu\rangle\) 1.7%
Total 10.1%

(b) Combinations of transmitted states that could reveal Alice’s polarization alignment through single detections. Another 12.8% of states could be used similarly to infer Bob’s polarization alignment. These add up to 25.5% of transmitted states which were previously discarded, but could be recycled and used. In comparison, only 10.1% (table 1(a)) could contribute to the secret key.

Table 1: Overview of measurements in MDI-QKD. Here we assume two decoy state implementation, with signal intensity \(\mu\) and decoy intensities \(\nu\) and \(\omega\), where \(\omega\) is close to vacuum. Intensity probabilities \(P_\mu = 0.52\), \(P_\nu = 0.33\) and \(P_\omega = 0.15\) are used for probability calculations.

Fig. 1: Monitoring polarization alignment over 40 km of unisolated fibre (a) without and (b) with compensation.

(a) Significant Polarization drifts were observed which call for active compensation in fibre-based QKD systems. (b) Polarization is maintained using our real-time novel polarization compensation scheme during an MDI-QKD experiment. The overall QBER for this three-hour session is below 3%.

In summary, we have proposed and implemented a novel polarization compensation scheme that recycles some of the discarded detections in MDI-QKD. This scheme runs independently for each user, in real-time in parallel to the key sharing. Since it does not decrease the key sharing cycle or require additional resources, this compensation scheme paves the way for polarization encoding MDI-QKD network.

We thank NSERC, CFI, ORF, MITACS, Royal Bank of Canada, Huawei Technology Canada and the U. of Toronto start-up funding for financial support.

References
1. Lo, Hoi-Kwong, Marcos Curty, and Bing Qi. Physical review letters 108.13 (2012): 130503.
2. See, for example, Wei, Kejin, et al. Physical Review X 10.3 (2020): 031030.
3. See, for example, Da Silva, T. Ferreira, et al. Physical Review A 88.5 (2013): 052303.
4. See, for example, Pugh, Christopher J., et al. Quantum Science and Technology 2.2 (2017): 024009.
5. Ding, Yu-Yang, et al. Optics letters 42.6 (2017): 1023-1026.
6. Xu, Feihu, et al. New Journal of Physics 15.11 (2013): 113007.