MDI-QKD with resource-efficient polarization compensation

Olinka Bedroya,[1,*] Chenyang Li,[2,3], Wenyuan Wang [3], Jianyong Hu[2], Hoi-Kwong Lo[1,2,3,4] and Li Qian[2]

[1] *Centre for Quantum Information and Quantum Control, Dept. of Physics, University of Toronto, Toronto, Ontario, M5S 3G4, Canada*
[2] *Centre for Quantum Information and Quantum Control, Dept. of Electrical & Computer Engineering, University of Toronto, Toronto, Ontario, M5S 3G4, Canada*
[3] *Department of Physics, University of Hong Kong, Pokfulam, Hong Kong*
[4] *Quantum Bridge Technolgies, Inc., (QBT), 100 College St, Toronto, ON M5G 1L5, Canada.*
[*] *o.bedroya@mail.utoronto.ca*

Abstract: We implemented MDI-QKD with a novel polarization compensation scheme using discarded bits without reducing the key-sharing cycle or demanding additional resources. Polarization drift was maintained below 0.13 rad over a 40 km unisolated fibre spool for four hours, and the average secret key rate generated was 7.45×10^{-6} bits per pulse.

Quantum key distribution (QKD) is information-theoretically secure based on the laws of quantum physics. Although QKD is theoretically secure, unfortunately, experimental implementations do not perfectly satisfy the theoretical assumptions made in the security proof. So far, the detection side has proven to be the most vulnerable part, attracting most of the attacks (for a review, see [1]). Measurement-device-independent QKD (MDI-QKD) scheme was proposed [2] to remedy this situation and close all the loopholes on the detection side. In MDI-QKD, each of the two users (Alice and Bob) who want to share a secret key prepares and transmits a state to an untrusted third party (Charlie) who performs a Bell-state measurement on the received states. Numerous different implementations of MDI-QKD have verified its feasibility with current technology. In running the MDI-QKD, we chose to use polarization encoding to encrypt data on the qubits since polarization state preparation and measurement are straightforward. However, polarization suffers in fibre-based communication due to the fibre's birefringence, and active compensation is needed. Different methods have been proposed for compensating for polarization and preserving the transmitted information through the channel. However, in available QKD literature, compensation always comes at a cost. The drawbacks fall into one of three categories[1]: (1) The key sharing needs to be interrupted (e.g. [4]) (2) Some additional resource is required (e.g. to multiplex reference polarization pulses with the signal [5]) (3) A fraction of quantum pulses is sacrificed for tomography (e.g. [6]).

We propose and implement a novel polarization compensation scheme that avoids all the above drawbacks by recycling some of the MDI-QKD's discarded detections. The security of MDI-QKD is based on the Bell state measurement, and specific coinciding detections mark a successful Bell state projection. These coincidences are collected for key distribution, and all single events are discarded. Additionally, detection events associated with decoy intensities [7] do not contribute to the key generation and are discarded. In decoy-state QKD, quite often three different intensity setting μ, ν and ω are used and ω is often set to be a vacuum state as it allows the users to estimate the background rate. When one user sends a vacuum decoy state, the detection result provides direct information about the polarization state prepared and sent by the other user. The main idea of our scheme is to use the single measurements corresponding to these transmitted states to actively evaluate the polarization drift based on singles' error rates and run compensation independently for each user. For example, given our experimental parameters, we observe that 25.5% of transmitted states that were previously discarded could be recycled and used to estimate the polarization misalignment of the user's bases to Charlie's bases. To put this number in perspective, only 3.4% of transmitted states could contribute to the secret key.

We implement our scheme for polarization encoding MDI-QKD which is the most demanding in polarization alignment as it requires the alignment of two polarization bases. We slightly modified the measurement node to simultaneously track and maintain the alignment of each user's rectilinear and diagonal bases. In the original MDI-QKD paper, the Bell-state measurement implementation includes two polarization beam splitters projecting onto the rectilinear basis. However, this is insufficient for polarization encoding MDI-QKD where users' two polarization bases should be aligned. Traditionally at least two polarization controllers, one before each polarization

[1] We are aware of only one exception to the abovementioned classification where real-time compensation was implemented based on the data revealed in the privacy amplification [3]. Unfortunately, this scheme does not apply to MDI-QKD as privacy amplification is based on coincidences, and the polarization drift of individual users cannot be inferred from it.

beam splitter, should be used to align the optical setup for Bell state measurement. A slight modification to the measurement setup using these two polarization controllers can address this challenge[2]. There is no need to add additional controllers to the experimental setup. Our solution is the simultaneous rotation of the axes of both polarization beam splitters, which does not reduce the key rate. This modification to the measurement setup allows us to infer the polarization drift in both bases using the aforementioned single detections.

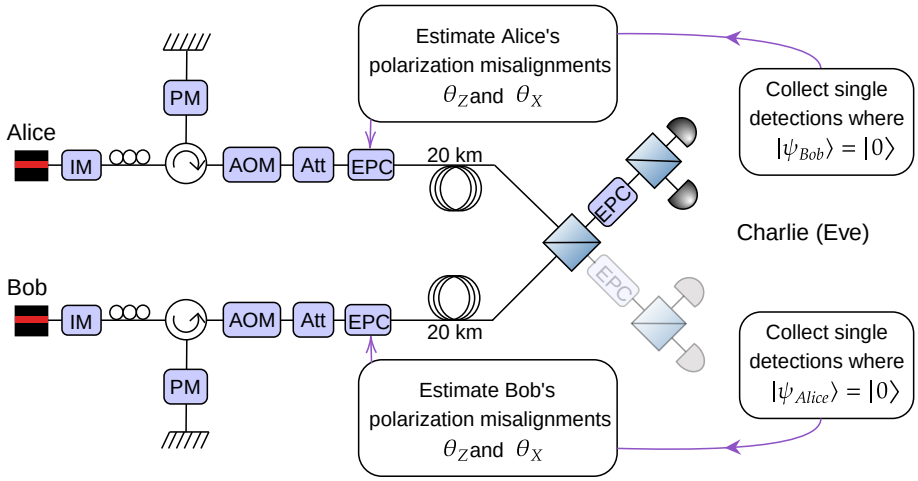

Fig. 1: The experimental setup of MDI-QKD with real-time polarization compensation: Attenuator (Att), Intensity Modulator (IM), Phase Modulator (PM), Electronic Polarization Controller (EPC), Acousto-Optic Modulator (AOM). Charlie announces the estimated polarization misalignment of each user based on the error rate of single detections when the other user transmits a vacuum decoy state. Alice and Bob locally and independently run the compensation. Both compensation and key generation were achieved without the use of the faded detection system; however, the detectors can be added to improve the key rate further.

Let us describe our compensation scheme as a control loop as shown in Figure 1. In that case, the system is the fibre spool between the user and measurement node, the feedback measurements are the polarization misalignments of two bases θ_Z and θ_X estimated based on the single detections (as $\arcsin(\sqrt{\text{error rate}})$), the input error signal to the controller is their average with the desired value zero, and the control actuator is an electronic polarization controller. Ordinarily, after Charlie announces the successful Bell state measurements in MDI-QKD, Alice and Bob announce their bases and intensity settings for sifting and post-processing. Furthermore, we require Charlie not to discard the single detections immediately and announce the single detections when one user has transmitted a vacuum. Then, we request Alice and Bob to reveal their transmitted polarizations corresponding to those timestamps so that Charlie can calculate and announce the polarization misalignments. Note that this information does not correspond to coincidences and does not compromise the key's secrecy. The compensation will launch if the misalignment exceeds a preset threshold. Three tunable parameters influence the performance of the compensation scheme which we optimized based on the experimental setup: the data collection time, the ratio of polarization rotation to the measured misalignment for compensation, and the threshold to start the compensation.

In our experimental setup (Figure 1), each user is connected to the central measurement node via a 20 km fibre spool. The fibre has a 250 μm standard acrylate buffer layer and is exposed to the lab environment without thermal or vibrational insulation. The average polarization drift was successfully maintained below 0.13 rad over 40 km of spooled fibres left exposed and without isolation throughout a four-hour run. We achieved an average key rate of 7.45×10^{-6} bits per pulse. The results are presented in table 1. Further details of our work can be found in [8].

[2]One approach is to rotate the axis of one of the polarization beam splitters in the measurement setup. This simple solution has a drawback when using weak coherent pulses; in order to keep the QBER due to multiphoton pulses low, one of the distinguishable Bell states must be forgone, which reduces the key rate by half.

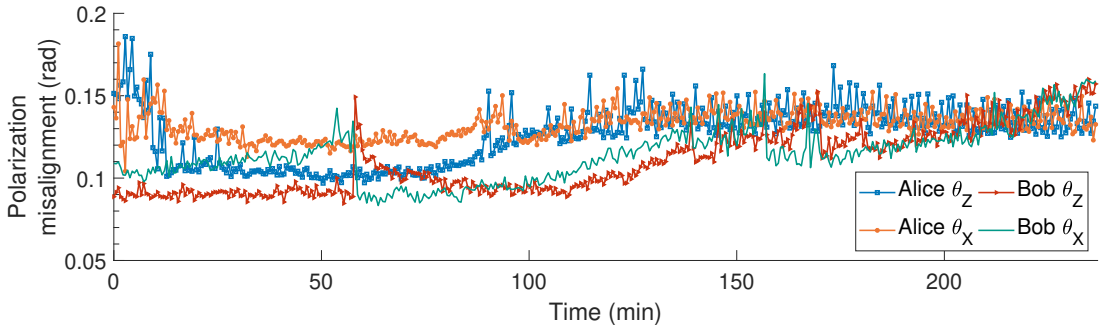

Fig. 2: Real-time tracking of polarization misalignment of the two users for an MDI-QKD session over 40 km of unisolated fibre with polarization compensation. The average misalignment is maintained below 0.13 rad. The average misalignment is maintained below 0.13 rad. The average QBER is 3.8%, and we achieved an average key rate of 7.45×10^{-6} bits per pulse.

(a)

$Q_Z{}^{\mu\mu}$	$E_Z{}^{\mu\mu}$	$Y_z{}^{11,L}$	$Y_x{}^{11,L}$	$e_x{}^{11,U}$	R_∞ (bit per pulse)	Alice's average misalignment	Bob's average misalignment
3.00×10^{-5}	0.038	8.02×10^{-4}	9.91×10^{-4}	0.148	5.94×10^{-6}	0.126rad	0.110 rad

(b)

$Q_X{}^{\mu\mu}$	$E_X{}^{\mu\mu}$	$Y_z{}^{11,L}$	$Y_x{}^{11,L}$	$e_x{}^{11,U}$	R_∞ (bit per pulse)	Alice's average misalignment	Bob's average misalignment
3.19×10^{-5}	0.038	9.82×10^{-4}	8.17×10^{-4}	0.117	8.96×10^{-6}	0.132 rad	0.115 rad

Table 1: Asymptotic key rate, the average polarization misalignments and other parameters corresponding to the half of the experiment where the Bell state measurement projects unto (a) Z basis and (b) X basis

In summary, we proposed and implemented a novel polarization compensation scheme in the MDI-QKD system that recycles a portion of the discarded detection events corresponding to decoy intensities. This compensation can be done in real-time without interruption, extra equipment, or sacrificing any quantum signal intended for key sharing. Since low key rates and cost are the two most pressing challenges preventing the wide adoption of QKD systems, avoiding these drawbacks is a step towards making QKD commercially viable.

Additionally, we note that our scheme is favourable for MDI-QKD network implementations for two reasons: (1) It allows us to retain a simple structure for user nodes without adding any additional equipment for compensation. In an ideal MDI-QKD network, it is beneficial to keep the nodes as simple as possible so that adding a user could be feasible in terms of cost and practicality. (2) Our scheme does not interrupt or reduce key-sharing between the detection node and any of the users. This is especially important for MDI-QKD networks where the detection system is shared with a number of users, and the key-sharing time allocated to each user is limited and thus valuable.

We thank NSERC, CFI, ORF, MITACS, US ONR, Royal Bank of Canada and Huawei Technologies Canada Inc., and the University of Hong Kong start-up grant for financial support.

References

[1] Feihu Xu et al. Secure quantum key distribution with realistic devices. *Revs. Mod. Phys.*, 92(2):025002, 2020.

[2] Hoi-Kwong Lo et al. Measurement-device-independent quantum key distribution. *Phys. Rev. Lett.*, 108:130503, Mar 2012.

[3] Yu-Yang Ding et al. Polarization-basis tracking scheme for quantum key distribution using revealed sifted key bits. *Opt. Lett.*, 42(6):1023–1026, 2017.

[4] Yang Liu et al. Decoy-state quantum key distribution with polarized photons over 200 km. *Opt. Express*, 18(8):8587–8594, 2010.

[5] Christopher Pugh et al. Airborne demonstration of a quantum key distribution receiver payload. *Quantum Sci. Technol.*, 2(2):024009, 2017.

[6] T Ferreira Da Silva et al. Proof-of-principle demonstration of measurement-device-independent quantum key distribution using polarization qubits. *Phys. Rev. A*, 88(5):052303, 2013.

[7] Hoi-Kwong Lo et al. Decoy state quantum key distribution. *Phys. Rev. Lett.*, 94(23):230504, 2005.

[8] Olinka Bedroya et al. Resource-Efficient Real-Time Polarization Compensation for MDI-QKD with Rejected Data. *preprint arXiv:2209.02707 [quant-ph]*, 2022.