Response to review of manuscript ID #437896: Y. Shi et al.: "Fibre polarization state compensation in entanglement-based quantum key distribution"

Dear Editor,

We appreciate the reviewer's response and would like to address his/her comments as below:

1, A brief description is added in the abstract (line 14) to summarize the implementation of the polarisation compensation technique in a QKD setup.

2, "Unconditionally secure communication" is replaced with "Information-theoretic secure communication" in line 19.

3, To address the reviewer's concern, we would like to point out that the signal and idler photons did undergo two different fibre paths in our work (line 114). This technique makes use of the rotational invariance of the polarisation entangled state of photon pairs and does not require the two fibre channels to be drifting at the same rate.

4, In this work we are using a continuous-wave pump laser, hence the entangled photon pairs are generated at random times and there is no applicable clock rate in this context. However, a fair comparison could be made to the coincidence rate and the sifted key rate in our entanglement QKD setup, which is stated in the 4th paragraph of section 4 (line 143 & 144). For the long term behaviour of the QKD setup, a short description is added to the end of section 4 (line 162), as well as a reference to our previous work (line 164).

5, The typo in section 4 is corrected (line 134).

6, In Ref.[23], qubits were encoded in polarisation states of weak coherent pulses from a DFB laser. While the photon bandwidth is not specified in that article, we would assume it to be much smaller than the bandwidth of photons from a SPDC process, which is about 20nm in our work. This larger photon bandwidth makes our entanglement QKD setup more susceptible to dispersion effects of the optical fibre and therefore leads to a higher QBER. We add a specification of our entangled photon bandwidth in the first paragraph of section 2 (line 77). The last paragraph of section 4 is rephrased to summarize the possible contributions of the high QBER value (line 163).

7, We would like to point out that both Ref.[23] and Ref.[24] are using Prepare & Measure protocols which only requires sending weak coherent pulses across a single optical fibre channel. Both works operated at a relative high pulse repetition rate (2.5MHz and 50MHz for Ref.[23] and Ref.[24] respectively) which results in a lower poissonian noise in the estimated QBER and thus a higher bandwidth of the feedback loop.

While our polarisation compensation scheme is also based on minimization of QBER, we demonstrated that our compensation technique can be implemented in an entanglement-based QKD system which contains two different fiber channels. We also adopted a stochastic search algorithm which is more robust aganist noise in the estimated QBER value and is suitable for entanglement-based QKD where the photon coincidence rate is typically much lower than the clock rate of Prepare & Measure systems. As stated in the last paragraph of section 5 (line 177), our method is more suitable for fibre-QKD with slowly drifting polarisation noise with limited accuracy in QBER estimation while the methods in Ref.[23] and [24] can be afforded in a scenario with faster polarisation noise.

The reviewer also commented on Fig.3(b) and (c) of the draft regarding the effectiveness of the compensation around the 15 minutes mark. We would like to point out that the small increase of QBER from 7% to about 9% only leads to a LCVR voltage search range of about 16mV which is small compared to the full operating range. That being said, one can still observe a noticeable ripple of the LCVR voltages around the 15 minutes mark, which later converges to a more constant value at the 20 minutes mark.

With this, we hope to have addressed the points raised in the review, and are looking forward for your reply.

With Best Regards on behalf of all authors,

Christian Kurtsiefer