High performance reference-frame-independent quantum key distribution based on passive decoy-state

Yang Xue1,2, Guan-jie Fan-yuan2, Wei Chen2,*, Lei Shi1,∗

Information and Navigation College, Air Force Engineering University, Xi’an
CAS Key Laboratory of Quantum Information, University of Science and Technology of China, Hefei

1 Motivation

- Reference-frame-independent (RFI) QKD is insensitive to relative rotations between Alice and Bob.
- Passive decoy-state method can reduce the risk of side-channel loopholes caused by imperfect active modulation.
- Imperfections of single-photon detectors in passive scheme may impair the SKR performance.

2 Model

- Weak coherent pulse-based implementation generates new photon distributions:

3 Mathematical Simulation

<table>
<thead>
<tr>
<th>ηd</th>
<th>p_d</th>
<th>f</th>
<th>τ_c</th>
<th>p_h</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.12</td>
<td>6×10^{-7}</td>
<td>1.16</td>
<td>50%</td>
<td>0.9</td>
</tr>
</tbody>
</table>

- Better reference frame deviation tolerance
- Comparable SKR with the active scheme
- Compatibility of untimely detection events.

By introducing the heralding efficiency \( P_h \), we divide the passively generated signals into: \( P_h P_c \) and \( P_h P_c + (1 - P_h)P_d \). \( P_h = 0 \) means that all heralding information is lost and the passive decoy-state method is not completed, \( 0 < P_h < 1 \) means that some pulses are not timely detected and the corresponding heralded signals contain three kinds of intensities. These intensities could be adopted into the two-decoy method, which is advantageous to higher SKR.

In conclusion, a universal model for the passive decoy RFI-QKD has been developed to incorporate the abnormal heralding events due to system defects. With this model the non-ideal features of Alice’s SPD could be better reflected. It can be derived by specific parameters such as the system repetition frequency, the dead-time and gate width of SPD. Our work could further provides beneficial reference for designing high-performance RFI-QKD systems.

Conclusions

References


We sincerely acknowledge the helpful discussion of F-Y. Lu and T. Jun. This work has been financially supported by the National Key Research and Development Program of China (2018YFA0306400), the National Science Foundation of China (61627820, 61971430).

E-mail: 18629631196@163.com