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

Yang Xue[1,2], *Guan-jie Fan-yuan*[2], *Wei Chen*[2,*], *Lei Shi*[1,*]

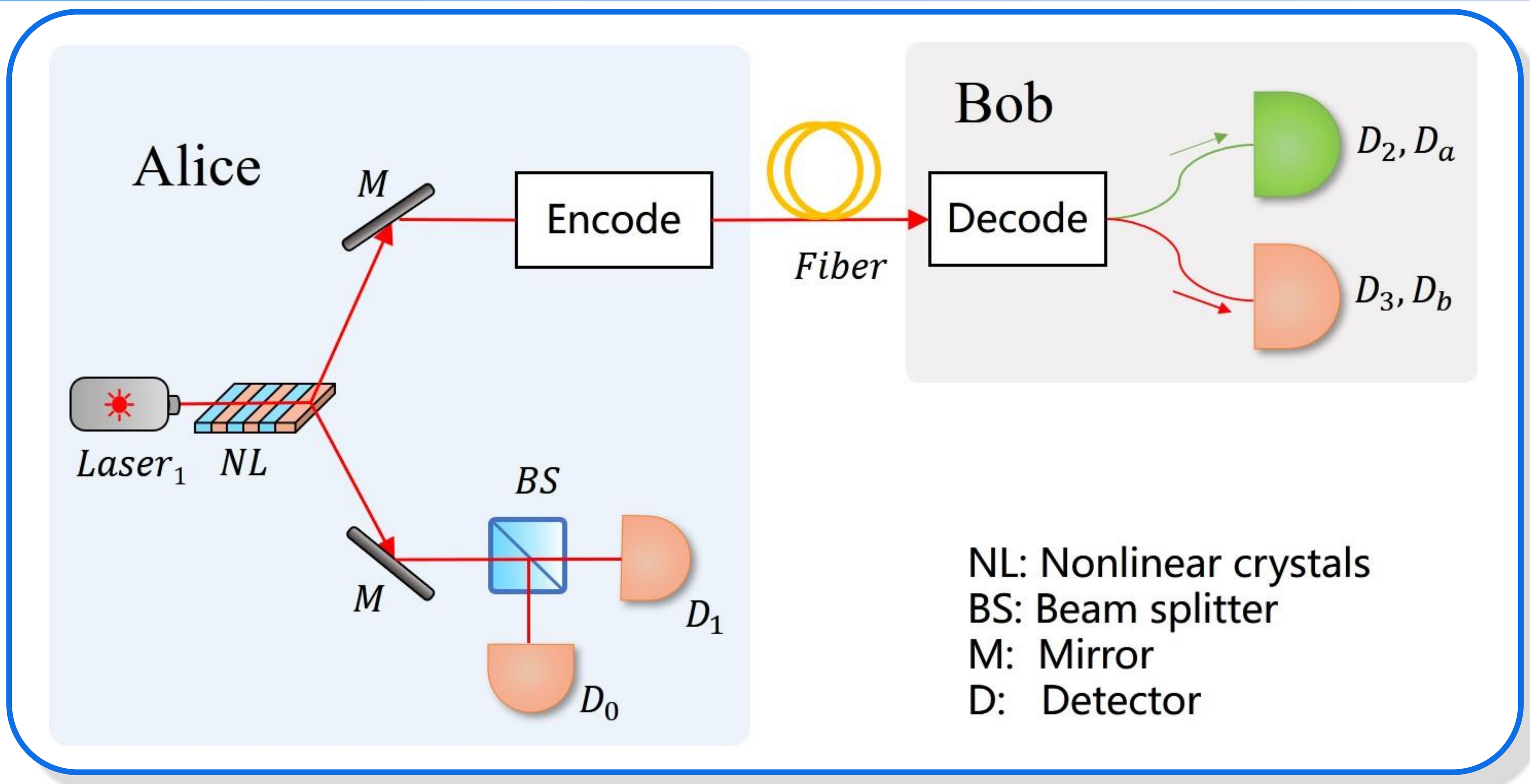
Information and Navigation College, Air Force Engineering University, Xi'an

CAS Key Laboratory of Quantum Information, University of Science and Technology of China, Hefei

① Motivation

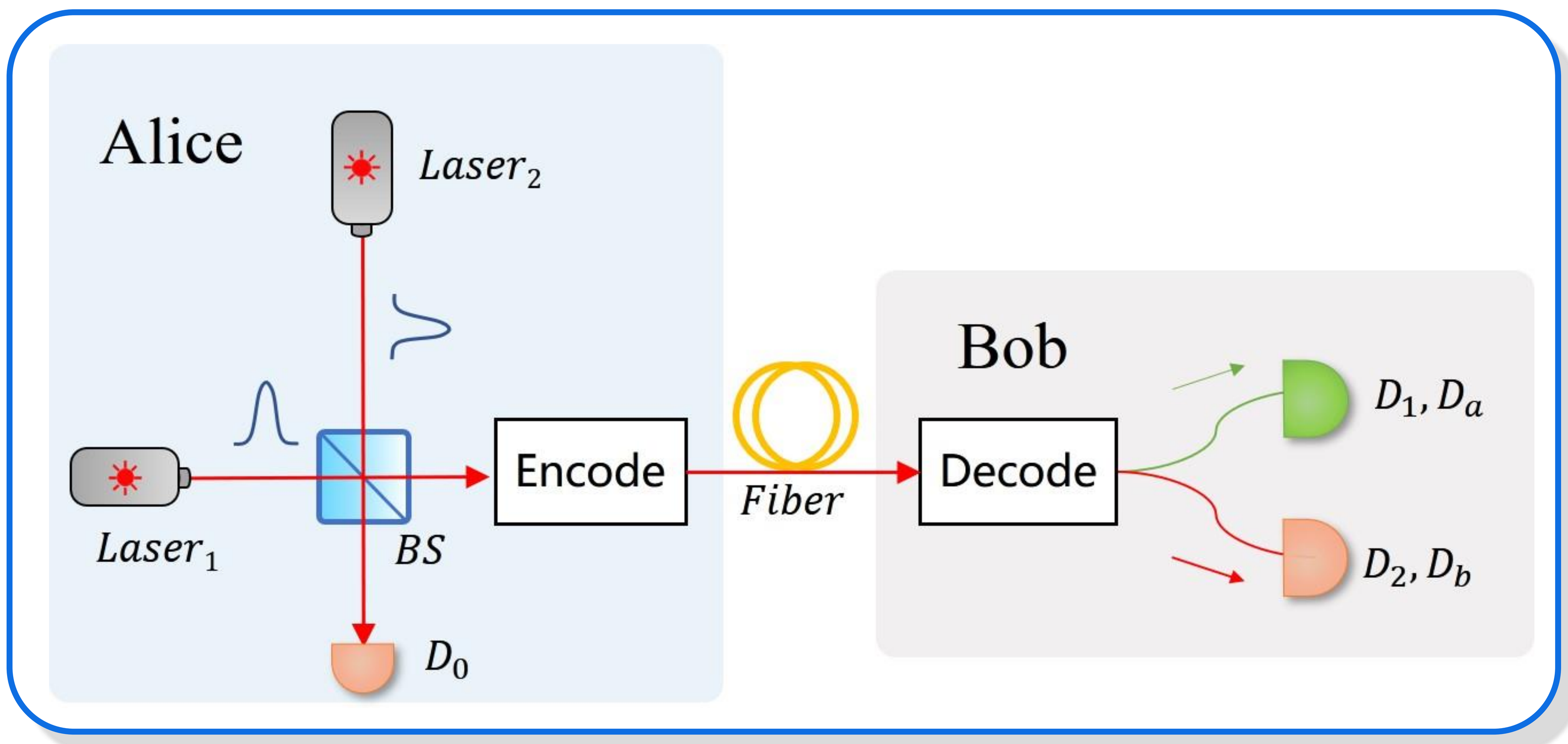
- Reference-frame-independent (RFI) QKD is insensitive to relative rotations between Alice and Bob.
- Passive decoy-state method can reduce the risk of side-channel loopholes caused by imperfect active modulation.
- Imperfections of single-photon detectors in passive scheme may impair the SKR performance.

Parametric down conversion-based scheme is not cost-effective
New model is proposed to incorporate non-ideal detection events



- Low efficiency
- High cost

② Model



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

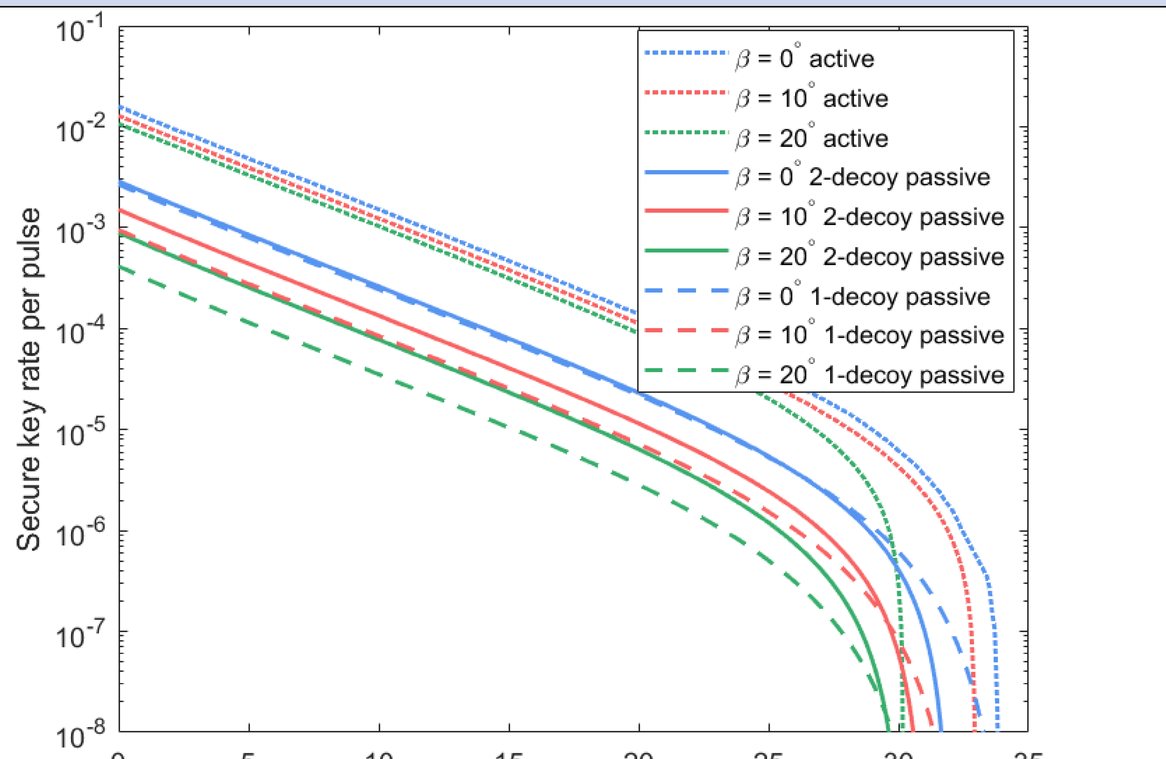
By introducing the heralding efficiency P_h , we divide the passively generated signals into: $P_h P_n^c$ and $P_h P_n^{\bar{c}} + (1 - P_h) P_n^t$. $P_h = 0$ means that all heralding information is lost and the passive decoy-state method is not completed, $0 < P_h < 1$ means that some pulses are not 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.

$$p_n^t = \frac{(t_c v)^n}{n!} \frac{1}{2\pi} \int_0^{2\pi} \gamma^n e^{-t_c v \gamma} d\theta \qquad p_n^{\bar{c}} = p_n^t - p_n^c$$

$$p_n^c = (1 - p_d) \frac{(t_c v)^n e^{-\eta_d v}}{n!} \frac{1}{2\pi} \int_0^{2\pi} \gamma^n e^{-v\gamma(t_c - \eta_d)} d\theta$$

③ Mathematical Simulation

η_d	p_d	f	t_c	p_h
0.12	6×10^{-7}	1.16	50%	0.9



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

Conclusions

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.

References

[1]. Phys.Rev.Appl.**12**,064044 (2019).
[2]. Phys.Rev.A. **102**, 062602 (2020).
[3]. Phys.Rev.A. **89**, 052325 (2014).
[4]. Phys.Rev.A. **81**, 022310 (2010).
[5]. Chin.Phys.B. **29**, 070303 (2020).

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