Enhancing the Secure Key Rate of Quantum Key Distribution using Realistic Quantum Dot based Single Photon Sources

Y. Bloom[1,†,*], **Y. Ordan**[1,†], **T. Levin**[1], **K. Sulimany**[1], **E.G. Bowes**[3], **J.A. Hollingsworth**[3], **R. Rapaport**[1,2]

[1]Racah Institute of Physics, The Hebrew University of Jerusalem, Jerusalem, 9190401, Israel
[2]The Center for Nanoscience and Nanotechnology, The Hebrew University of Jerusalem, Jerusalem 9190401, Israel
[3]CINT, Los Alamos National Laboratory, Los Alamos, New Mexico, 87545, USA
[†]These authors contributed equally.

The original proposal of quantum key distribution (QKD) was based on ideal single photon sources, which 40 years later, are still challenging to develop. Therefore, the development of decoy state protocols using weak coherent states (WCS) from lasers, set the frontier in terms of secure key rates.

We propose and experimentally emulate two simple-to-implement protocols that allow practical, far from ideal sub-Poissonian photon sources to outperform state-of-the-art WCS [1]. By engineering the photon statistics of a quantum dot's biexciton-exciton (BX-X) cascade, we show that either a truncated decoy state protocol or a heralded purification protocol can be employed to achieve a significantly increased performance in terms of the maximal allowed channel loss for secure key creation, which can exceed that of WCS by more than 3dB.

This is a particularly attractive route to improve the performance of current QKD systems. We have shown that even room temperature, on-chip, compact, and easily integrated SPS devices, such as those based on gCQD coupled to nano-antennas [2, 3], are already well within the parameter range for superior performance over WCS with decoy states by employing either protocol. Both protocols have very simple requirements and their application is very general, thus we believe they can be employed efficiently on a vast range of sub-Poisson, quantum emitters, opening a practical and realistic way to implement novel photon sources with superior QKD performance, without the stringent requirements that hindered their practical integration into real-world QKD systems.

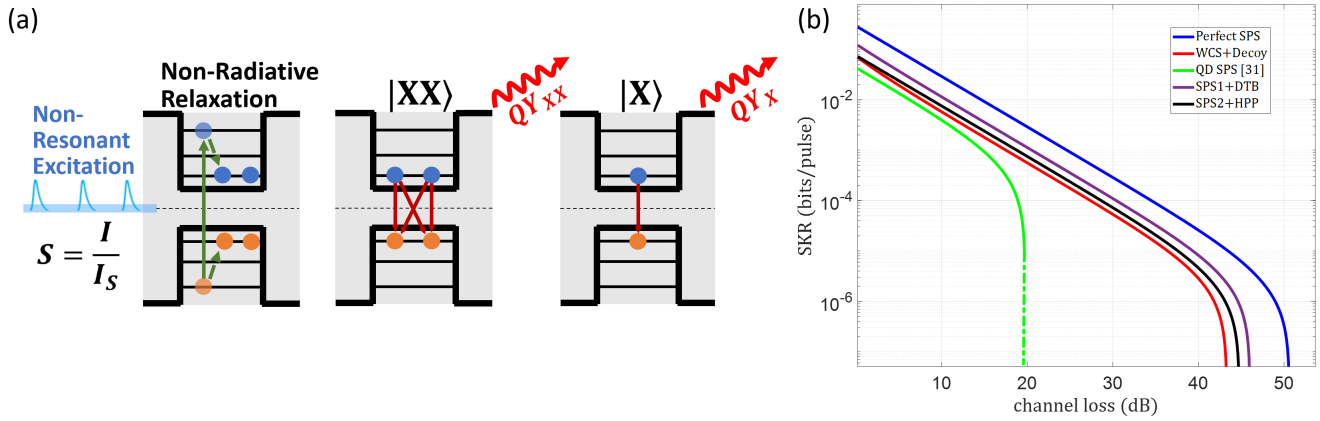

Figure 1: (a) Schematic of the BX-X cascade in an optically excited gCQD, using a non-resonant pulsed excitation with a normalized intensity $S = \frac{I}{I_S}$. (b) Secure key rate performance analysis for various sources, showing an improvement of our protocols (black, purple) compared to WCS with decoy states (red).

References

[1] Y Bloom[†], Y Ordan[†], T Levin, K Sulimany, JA Hollingsworth, R Rapaport, *arXiv Preprint* arXiv:2409.07939 (2024).

[2] A Nazarov[†], Y Bloom[†], B Lubotzky, H Abudayyeh, A Mildner, L Baldessarini, Y Shemla, EG Bowes, M Fleischer, JA Hollingsworth, R Rapaport, *ACS Photonics* **11**, 10, 4453-4460 (2024).

[3] H Abudayyeh, A Mildner, D Liran, B Lubotzky, L Luder, M Fleischer, R Rapaport, *ACS Nano* **15**, 11, 17384-17391 (2021).

*E-mail: yuval.bloom@mail.huji.ac.il