Fast and Simple One-Way High-Dimensional Quantum Key Distribution

Kfir Sulimany[1], Rom Dudkiewicz[2], Simcha Korenblit[1], Hagai S. Eisenberg[1], Yaron Bromberg[1], & Michael Ben-Or[2]

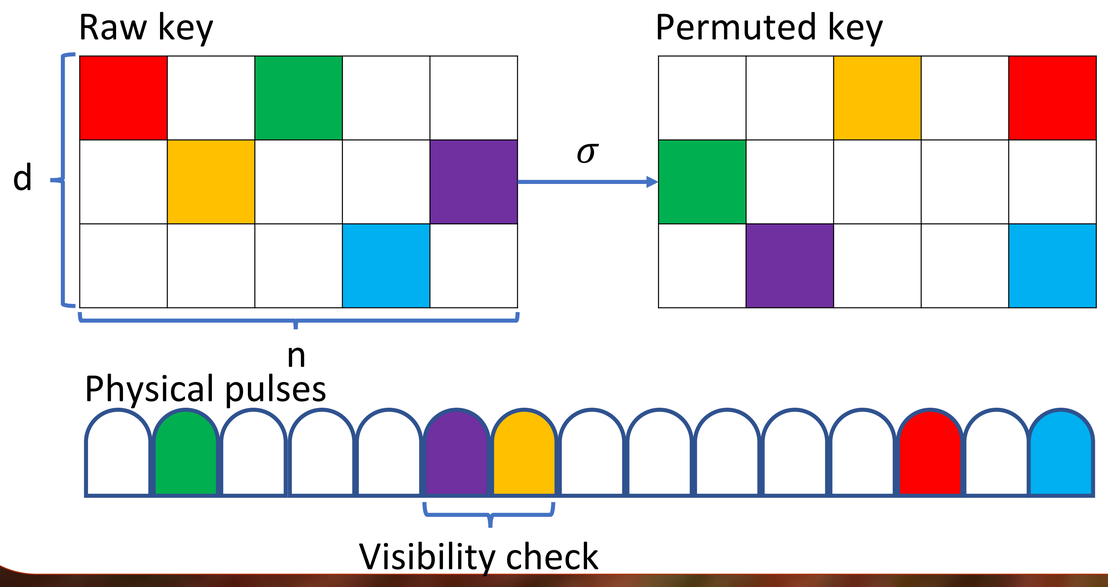
[1] Racah Institute of Physics, The Hebrew University of Jerusalem, Israel
[2] School of Computer Science & Engineering, The Hebrew University of Jerusalem, Israel

Abstract

- **High-dimensional quantum key distribution (HD-QKD)** protocols allow higher secure key rates and improved robustness to noise based on preparing a set of states belonging to a d-dimensional Hilbert space, called qudits [1,2].
- So far, the proposed protocols required additional experimental resources, thus raising the cost of practical high-dimensional systems and limiting their use [3,4].
- **We present a novel approach for HD-QKD with time-bin encoding, which can be implemented using a standard binary QKD system without any hardware modifications [5].** We analyze and demonstrate a novel scheme for fiber-based HD-QKD, exhibiting a two-fold enhancement of the secret key rate.

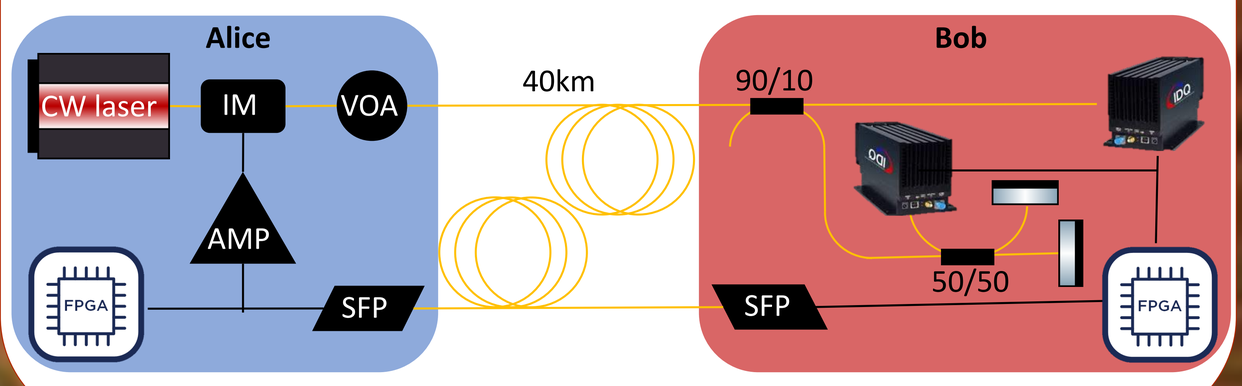
Protocol Scheme

- Our protocol is based on the **coherent one-way (COW)** QKD protocol, where the bit string is encoded in the arrival time of weak coherent laser pulses and the channel disturbance is monitored by measuring the visibility of the interference between consecutive pulses [6,7].
- Our extension to HD-QKD of the COW protocol:
  1. Encode the qudits of the **raw key** by a sequence of d time slots, where in each sequence only one time slot is populated, and the rest are empty.
  2. Group n sequences to a block and apply a random permutation (σ) to create a **permuted key** block.
  3. Convert the block to a sequence of **physical pulses**.
- The random permutation plays a key role as it guarantees that two successive occupied pulses can originate anywhere in the raw key block. This allows to bound Eve's information and extract a higher secure key rate, even though our monitoring interferometer probes the coherence of consecutive pulses only [5].



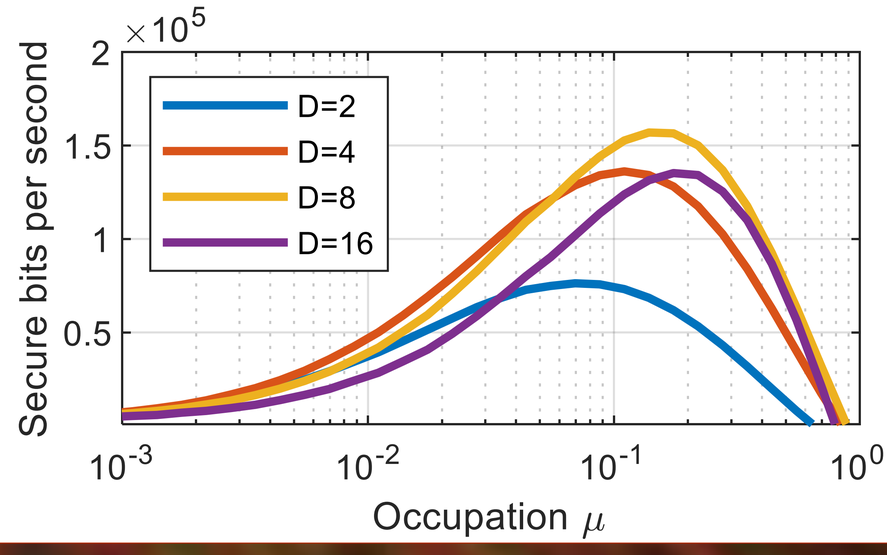
Experimental Demonstration

- The transmitter sends a train of weak coherent pulses that are prepared from a continuous wave laser emitting at λ=1550nm by an intensity modulator (IM) running at 500MHz. The pulses are attenuated to reach single photon level using a variable optical attenuator (VOA). To generate 200ps long pulses with random occupations of $\tau = 2ns$ long time-bins, we use a field programmable gate array (FPGA).
- To interfere consecutive pulses at the receiver's end, an unbalanced Michelson fiber-interferometer is installed, where we use Faraday mirrors to compensate for random polarization drifts in the fiber interferometer. We use single-photon avalanche detectors with 20% detection efficiency and 200ps timing resolution. The $4\mu s$ dead time of the detector limits the maximal raw key rate to $250kHz$.



Results

- We compute the **Holevo information** and find that the number of secure bits per photon could be significantly enhanced.
- We experimentally analyze the **secure bits per second** versus the occupations (μ) for different dimension sizes with our QKD system.
- An optimal secure bit rate is achieved for $d = 8$, resulting in more than a **two-fold increase in the secure bits rate**.



References

[1] H. Bechmann-Pasquinucci and W. Tittel, Physical Review A 61, 062308(2000).
[2] N. J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, PRL 88, 127902 (2002).
[3] Cozzolino, Daniele, et al. Advanced Quantum Technologies 2.12 (2019): 1900038.
[4] Islam, Nurul T., et al. Science advances 3.11 (2017): e1701491.
[5] Sulimany, Kfir, et al. arXiv preprint arXiv:2105.04733 (2021).
[6] Stucki, Damien, et al. Applied Physics Letters 87.19 (2005): 194108.
[7] Branciard, Cyril, Nicolas Gisin, and Valerio Scarani. New Journal of Physics 10.1 (2008): 013031.

For more information:

arXiv:2105.04733

This research was supported by the United States-Israel Binational Science Foundation (BSF) (Grant No. 2017694) and by the Israel Science Foundation (ISF) grant No. 2137/19. KS and YB acknowledge the support of the Israeli Council for Higher Education, the Israel National Quantum Initiative (INQI) and the Zuckerman STEM Leadership Program.

Conclusions and Outlook

- Our demonstration shows that the proposed HD-QKD extension of the COW protocol allows a significant improvement in the key generation rate as compared with the binary-encoding case.
- At the same time, no additional hardware is required to fully implement the protocol in standard two-dimensional systems.
- Our analysis predicts an improvement also for high-end QKD systems based on superconducting nanowire detectors.
- Therefore, our work paves the way towards a wider use of high-dimensional encoding in QKD.

MORTIMER B. ZUCKERMAN STEM LEADERSHIP PROGRAM

COUNCIL FOR HIGHER EDUCATION

BSF

ISRAEL SCIENCE FOUNDATION