High Dimensional Quantum Key Distribution System Using Structured Light

Muhammad Kamran, Muhammad Mubashir Khan and Tahir Malik
NED University of Engineering and Technology, Karachi, Pakistan.

Aim

Practical Implementation of HD QKD system based on higher dimension QKD protocol (KMB09).

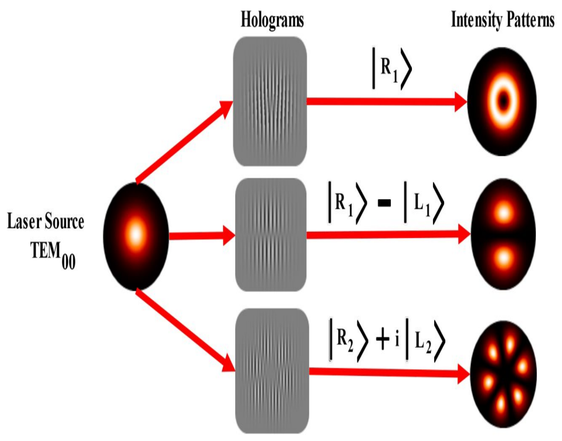
Basic Principles of QKD

Uncertainty Principle
– The state of a quantum system cannot be determined unless it is measured.

No Cloning Theorem
– Impossible to copy unknown pure quantum states.

Structured Light

- Light carrying orbital angular momentum (OAM) forms the structured light.
- Laguerre gaussian modes normally contain the OAM number associated with twist or rings.
- OAM modes can be directly created from laser using SLM driven by computer generated complex binary holograms.



Decoy State Scheme

- We also incorporate a decoy-state scheme to improve the QKD system efficiency on a secure transfer of secret keys.
- We utilized vacuum plus weak coherent pulses to avoid the Photon Number Splitting (PNS) attack.

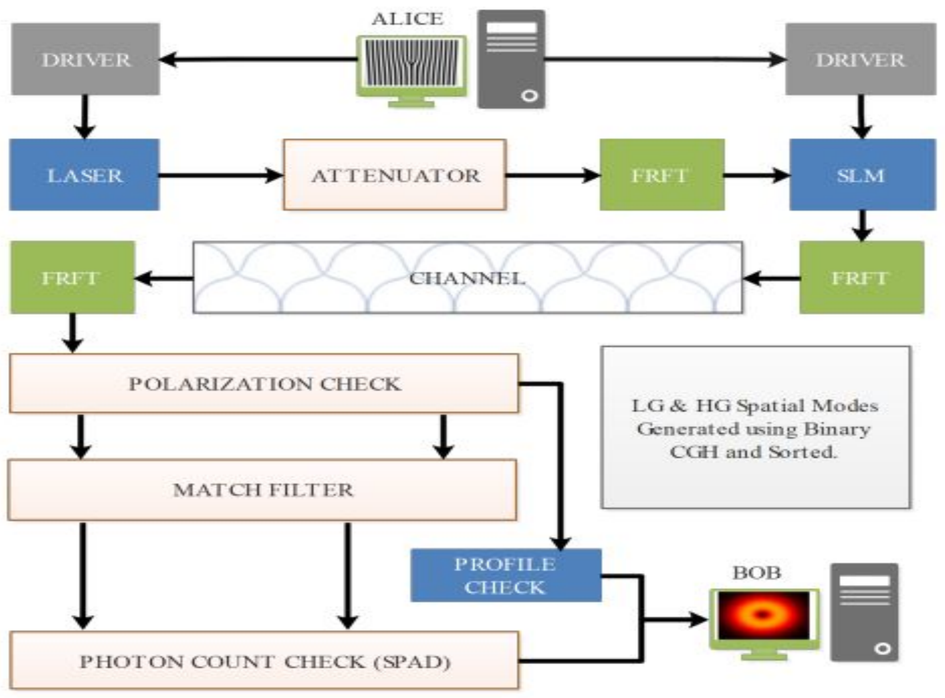
HD-QKD Protocol

- A high dimensional QKD protocol proposed in 2009 with two different eavesdropping error-rates.
  i. The Quantum Bit Error-rate (QBER).
  ii. The Index Transmission Error-rate (ITER).
- Bits are encoded in bases instead of dimensions.
- Improved eavesdropping detection.

Index By Alice	Measurement By Bob (bits)											
	$\|\tau_1\rangle$	$\|\tau_2\rangle$	$\|\tau_3\rangle$	$\|\tau_4\rangle$	...	$\|\tau_N\rangle$	$\|v_1\rangle$	$\|v_2\rangle$	$\|v_3\rangle$	$\|v_4\rangle$	...	$\|v_N\rangle$
1	×	1	1	1	...	1	×	0	0	0	...	0
2	1	×	1	1	...	1	0	×	0	0	...	0
3	1	1	×	1	...	1	0	0	×	0	...	0
4	1	1	1	×	...	1	0	0	0	×	...	0
...	...	...	...	...	...	...	...	...	...	...	...	...
N	1	1	1	1	...	×	0	0	0	0	...	×

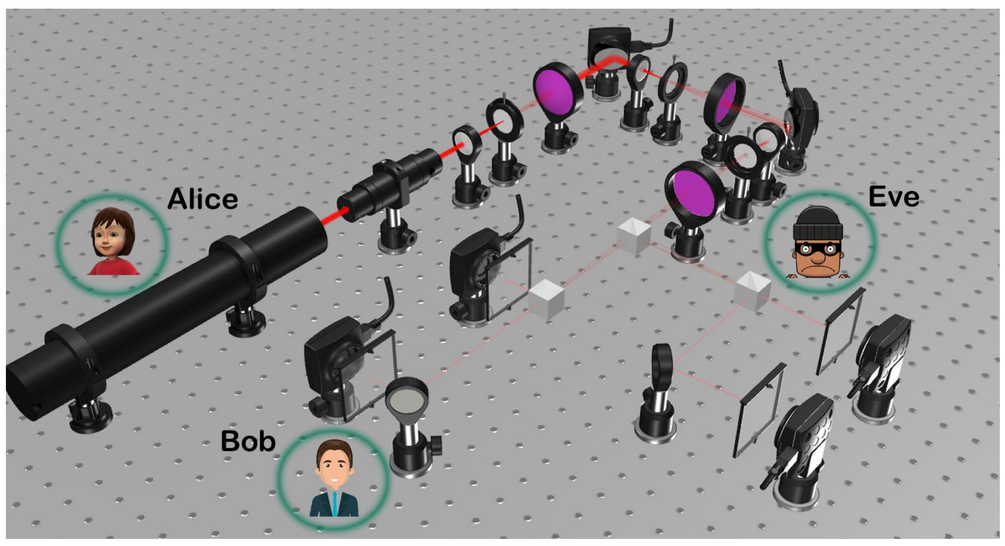
HD-QKD System Design

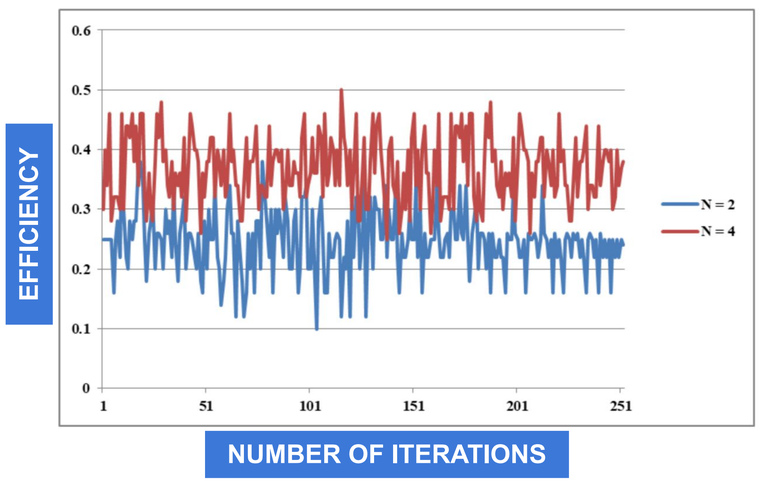
- QKD system comprises of Alice and Bob.
- Laser is the main source of photons having standard TEM_{00} Gaussian mode.
- Attenuator is used to limit μ per pulse.
- Beam expansion is done using 4f system.
- Spatial modulation is done with SLM by imposing holograms of LG modes.
- Higher order filtering is done using 4f system.
- First determine polarization of OAM mode.
- Second to use Match filter (SLM with fiber-coupler) for determining incoming photon mode carrying OAM.
- SPADs modules are used for photon counting.
- CMOS camera is used for profile checking.

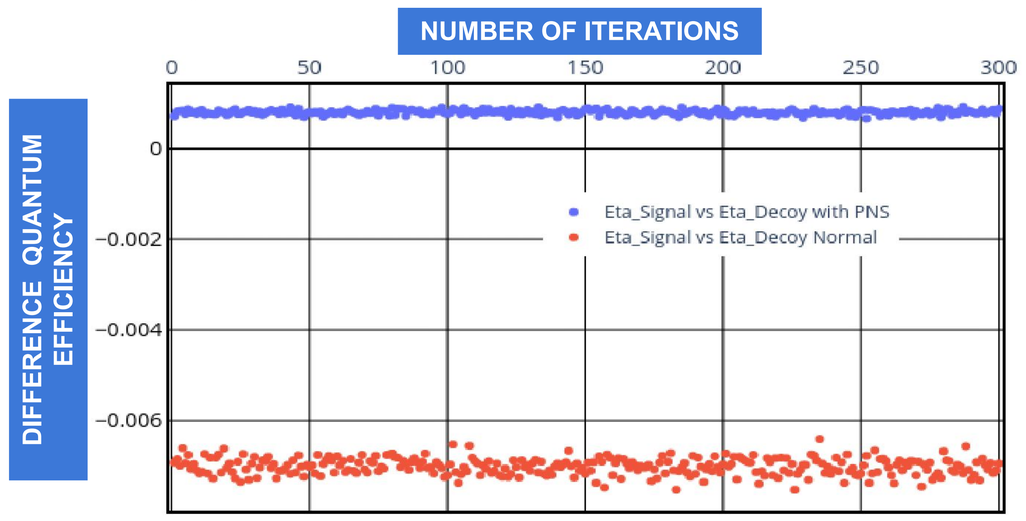


HD-QKD System Simulation

- Simulation is carried out on open source platform (python 3.7).
- SLM libraries and image processing (SSIM) schemes are mainly utilized in over-all simulation.
- Cartoon setup is developed using online 3D optical simulation tool.
- Graph shows the system simulation results in 2 and 4 dimensions in terms of efficiency and their absolute error w.r.t analytical results.







References

[1] Allen L, Beijersbergen MW, Spreeuw RJ, Woerdman JP. Orbital angular momentum of light and the transformation of Laguerre-Gaussian laser modes. Physical review A. 1992 Jun 1;45(11):8185.

[2] Khan, M.M., Murphy, M., Beige, A.: High error rate quantum key distribution for long-distance communication. New Journal of Physics 11 2009 063043.

[3] Hussain SS, Khan MM, Baig MM, Wang G. Numerical modelling of quantum key distribution system for KMB09 protocol. International Journal of Computer Science and Information Security. 2016 Aug 1;14(8):140.

[4] Forbes A. Structured light from lasers. Laser & Photonics Reviews. 2019 Nov;13(11):1900140.

[5] Cozzolino D, Bacco D, Da Lio B, Ingerslev K, Ding Y, Dalgaard K, Kristensen P, Galili M, Rottwitt K, Ramachandran S, Oxenløwe LK. Orbital angular momentum states enabling fiber-based high-dimensional quantum communication. Physical Review Applied. 2019 Jun 25;11(6):064058.

Future Research Challenges

- Handling of attacks using protocol error rates i.e., QBER & ITER.
- Analysis of QKD system efficiency due to turbulence in quantum channel.

Acknowledgement

We acknowledge support from NED University of Engineering & Technology, Karachi and Higher Education Commission of Pakistan to carry out this project.