High-Dimensional Quantum Key Distribution with decoy states using discrete-variable time-frequency states

Nurul T. Islam,[1] Clinton Cahall,[2] Andrés Aragoneses,[1] Charles Ci Wen Lim,[3] Michael S. Allman,[4] Varun Verma,[4] Sae Woo Nam,[4] J. Kim,[2] Daniel J. Gauthier[5]

[1]Department of Physics, Duke University, Durham, North Carolina 27708, USA
[2]Department of Electrical Engineering and the Fitzpatrick Institute for Photonics, Duke University, Durham, North Carolina 27708, USA
[3]Quantum Information Science Group, Computational Sciences and Engineering Division, Oak Ridge National Laboratory, Oak Ridge, TN 37831-6418, USA
[4]National Institute of Standards and Technology (NIST), 325 Broadway, Boulder, Colorado 80305, USA
[5]Department of Physics, The Ohio State University, 191 West Woodruff Ave., Columbus, Ohio 43210 USA
nti3@duke.edu

Quantum Key Distribution (QKD) is a provably secure communication technique that leverages the inherent uncertainty of quantum measurements to share a random string of key between two remote users (Alice and Bob) in the presence of an eavesdropper (Eve). Most of the current implementations of QKD are realized using qubit-based ($d = 2$) protocols that encode a maximum of one bit of information per photon. However, in practice, the number of extractable secure bits per transmitted photon is much smaller. This is due practical limitations such as loss in the quantum channel or the relatively long recovery time of single-photon detectors compared to the timing window used to prepare the quantum states. A well known solution to these problems involves encoding information in high-dimensional ($d > 2$) time-bin states. High-dimensional time-bin encoding schemes have the advantage that each photon can encode a maximum of $\log_2 d$ bits of information, thus increasing the photon efficiency to overcome detector saturation. In addition, these schemes are also known to tolerate higher quantum bit errors compared to the qubit-based protocols. Here, we report our findings of a high-dimensional ($d = 4$) time-bin encoding QKD scheme, where information is encoded by placing a sharply peaked single-photon wavepacket in one of the d temporal bins. A single-photon wavepacket in a distinct time bin represents a distinct letter in a communication alphabet. The presence of an eavesdropper is monitored by generating and detecting frequency states which consist of a single-photon wavepacket in a superposition of time-bins with distinct phase coefficients based on discrete Fourier transforms of the temporal states. In order to measure the spectrum of the single-photon frequency states, we realize a cascade of time-delay interferometers, where each level of the tree has a factor of two shorter delay. To the extent possible, we implement our system using commercially-available components (Fig. 1), where the temporal and frequency states are generated using electro-optic intensity modulators driven by a field programmable gate array (FPGA). The frequency states are measured using a tree of passively stabilized, thermally compensated time delay interferometers and low-jitter and low-dark count single-photon detectors. Currently, we measure an upper bound secure key rate, $0.5(\log_2 4 - 2H(Q))$, where $H(Q)$ is Shannon's entropy for $d = 4$, of ~ 500 KHz at 50 km equivalent loss (10 dB). The secure key rate is mostly limited by low efficiency ($\sim$1 %) of our detectors and should improve with higher efficiency detectors. We also analyze the security of the system using semi-definite programming and show that the protocol is secure against collective attacks. In addition, we show that the security of this protocol can be guaranteed with just one frequency state (Fig. 2), which greatly simplifies the experimental setup and make this protocol more practical.

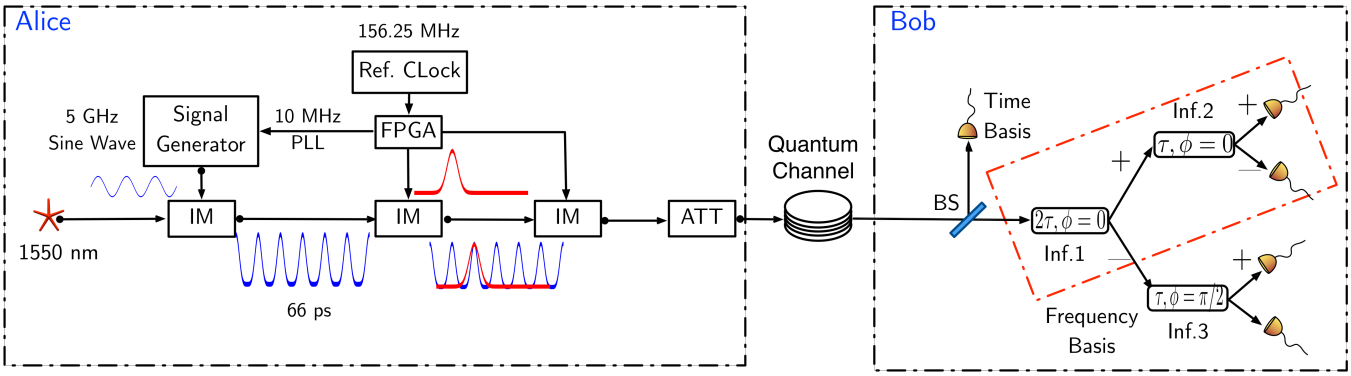

Figure 1: **Experimental Setup** On Alice's side, a 1550 nm cw laser is modulated into 66 ps wavepackets using an intensity modulator (IM) and a 5 GHz sine wave generator. A 10 GHz Field Programmable Gate Array (FPGA)-based pattern generator and a second intensity modulator are used to create all the temporal states and just one frequency state. A third intensity modulator is used to create the so-called decoy states before attenuating (ATT) the signals into single-photon wavepackets. The single-photon states are then transmitted through a quantum channel to Bob where he uses a beamsplitter (BS) to randomly perform either a temporal or frequency measurement. The temporal measurement is performed using a single-photon detector and a high resolution time-tagger. On the other hand, the frequency measurement is performed using a tree of three interferometers and single-photon detectors. The first interferometer (Inf. 1) has a free-spectral range of 1.25 GHz corresponding to a time-delay of 800 ps, while the second (Inf. 2) and third (Inf. 3) have free spectral ranges of 2.5 GHz corresponding to a time-delay of 400 ps. If only one frequency state is created, the detection of the frequency state can be performed with just one branch of the interferometric tree as indicated with the red box.

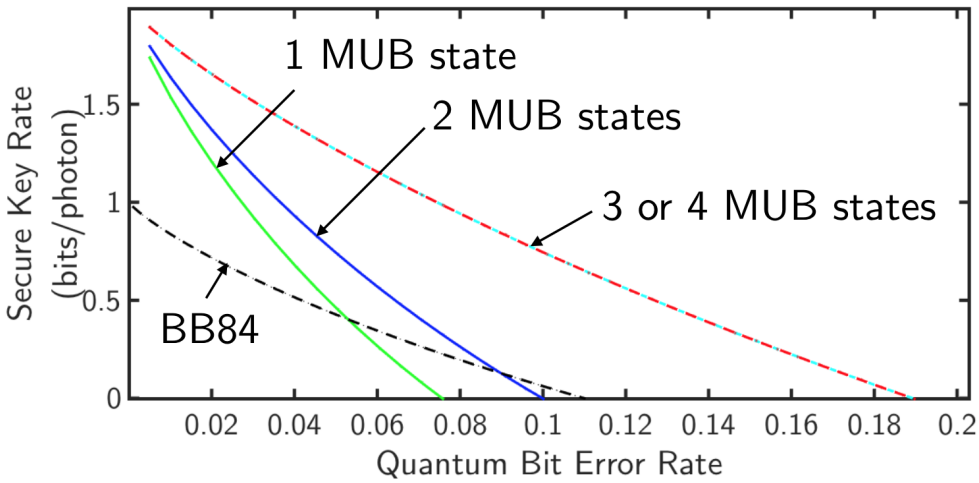

Figure 2: **Secure key rate as a function of quantum bit error rate** Based on our security analysis using semi-definite programming, we find that security of a two-basis high-dimensional protocol can be guaranteed with less than complete number of mutually unbiased basis (MUB) states. This greatly simplifies experimental setup and paves the way for a practical route to high-dimensional time-bin encoding schemes.