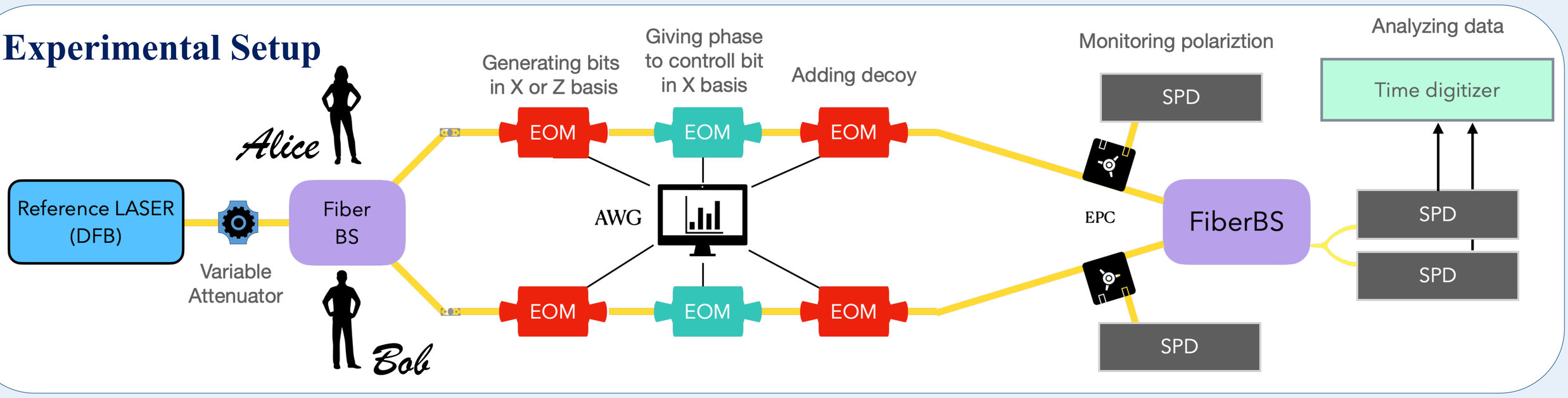
Toward Unhackable Quantum Network

Yen-An Shih, Tsung-Ying Tsai, and Chih-Sung Chuu*
Department of Physics, National Tsing Hua University, Hsinchu 30013, Taiwan and
Center for Quantum Technology, Hsinchu 30013, Taiwan
*Email: jumpsya@gmail.com

Abstract

Quantum key distribution (QKD) aims to provide an information theoretically secure way to distribute secret keys. However, practical devices may not follow the theoretical assumptions, which leaves a backdoor for eavesdropper to exploit. Single photon detectors are considered to be the most vulnerable part in QKD systems. Measurement device independent (MDI) protocol provides a way to remove all detector side channels by introducing an untrusted relay performing Bell-state measurement jointly on the prepared states. The relay can also serve as the central node of a quantum network, which allows quantum communication without trusted relay or point-to-point communication which is hard to scale up.

Experimental Setup



MDI-QKD Protocol

Alice prepares phase randomized weak coherent pulses (WCPs).

Bob prepares phase randomized weak coherent pulses (WCPs).

Alice chooses bit (0 or1), encoding basis (X or Z) and decoy amplitude (μ, ν, ω).

Bob chooses bit (0 or1), encoding basis (X or Z) and decoy amplitude (μ, ν, ω).

Alice and Bob send the pulse chain to Charley (an untrusted relay) to perform Bell state measurement.

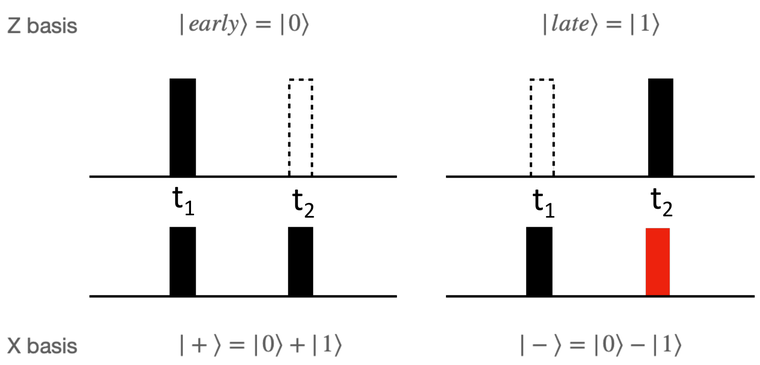
Charley announces the measurement results ($|\psi^+\rangle$ or $|\psi^-\rangle$).

Alice and Bob communicate with each other by authenticated public channel to compare their basis and decoy.

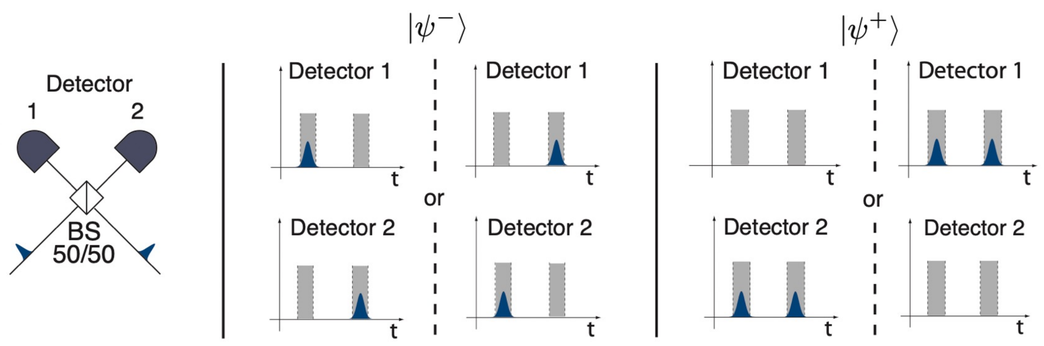
If the result is $|\psi^-\rangle$ from Charley, Bob always flip his bits.

If the result is $|\psi^+\rangle$ from Charley, Bob will flip his bits only when they choose Z basis.

Time-bin encoding

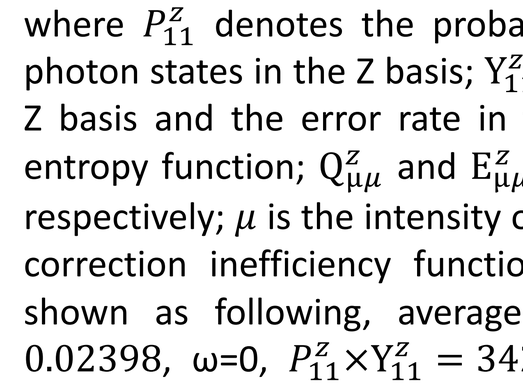


Weak coherent pulses (WCPs) in first (t_1) and second (t_2) time-bin represent bit 0 and bit 1, respectively, for the Z basis. WCPs prepared in t_1 and t_2 simultaneously with zero and π phase difference represent bit 0 and bit 1 for the X basis.

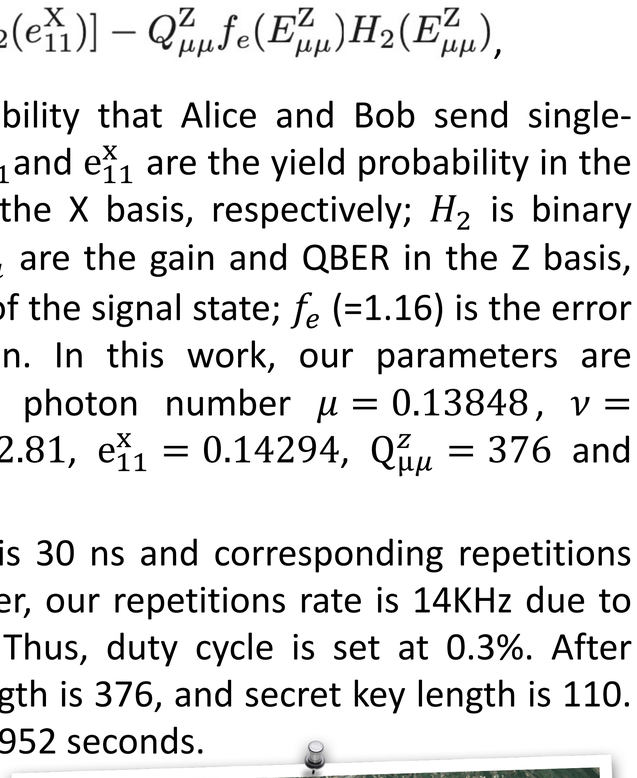


Here, we perform bell state measurements for time-bin qubits by checking coincidence on two detectors after a beam splitter.

Results



We first verify a high visibility HOM interference between two WCPs. The measured HOM dip is 52.45% ± 1%.



The secure key rate (R) of MDI-QKD is given by

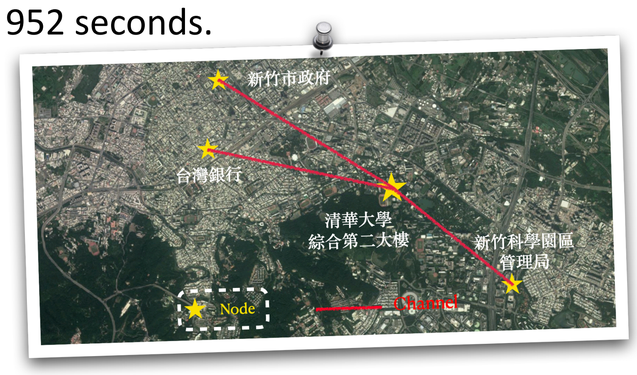
$$R \geq P_{11}^{Z} Y_{11}^{Z} [1 - H_2(e_{11}^{X})] - Q_{\mu\mu}^{Z} f_e(E_{\mu\mu}^{Z}) H_2(E_{\mu\mu}^{Z}),$$

where P_{11}^{z} denotes the probability that Alice and Bob send single-photon states in the Z basis; Y_{11}^{z} and e_{11}^{x} are the yield probability in the Z basis and the error rate in the X basis, respectively; H_2 is binary entropy function; $Q_{\mu\mu}^{z}$ and $E_{\mu\mu}^{z}$ are the gain and QBER in the Z basis, respectively; μ is the intensity of the signal state; f_e (=1.16) is the error correction inefficiency function. In this work, our parameters are shown as following, average photon number $\mu = 0.13848$, $\nu = 0.02398$, ω=0, $P_{11}^{z} \times Y_{11}^{z} = 342.81$, $e_{11}^{x} = 0.14294$, $Q_{\mu\mu}^{z} = 376$ and $E_{\mu\mu}^{z} = 0.00797$.

The square wave pulse width is 30 ns and corresponding repetitions rate should be 30MHz. However, our repetitions rate is 14KHz due to limit of detection dead time. Thus, duty cycle is set at 0.3%. After analyzing data, our raw key length is 376, and secret key length is 110. The total measurement time is 952 seconds.

Future work

We are planning to establish a star-like quantum network in Hsinchu City.



Reference

[1] Hoi-Kwong Lo, Marcos Curty, and Bing Qi, Phys. Rev. Lett. 108, 130503 (2012)
[2] Feihu Xu, He Xu, and Hoi-Kwong Lo, Phys. Rev. A 89, 052333 (2014)
[3] R. Valivarthi, I. Lucio-Martinez, A. Rubenok, P. Chan, F. Marsili, V. B. Verma, M. D. Shaw, J. A. Stern, J. A. Slater, D. Oblak, S. W. Nam, and W. Tittel, Optical Express. Vol 22, issue 20, pp 24497 (2014)