Multi-User Quantum Key Distribution with 148 Times Improvement in Key Rate

Cheng-Hong Liu*, Yen-An Shih, Tsung-Ying Tsai, Chih-Wen Kuo and Chih-Sung Chuu
Department of Physics, National Tsing Hua University, Hsinchu, 30013, Taiwan
and Center of Quantum Technology, Hsinchu, 30013, Taiwan
*Email: andy890608nike@gmail.com

Abstract

We present an enhanced quantum network communication protocol, building upon the standard MDI-QKD framework. This method achieves a 148 times improvement in the key rate and effectively mitigates quantum bit error rate from asymmetric channels. We demonstrate the new protocol in the laboratory and its progress towards commercial viability. Our aim is to develop practical quantum communication solutions for diverse users across various locations.

Why 7 intensity protocol?

In theory, QKD is secure. However, due to the equipment flaws, its practical implementation becomes insecure. To address these security concerns, various QKD protocols have been proposed.

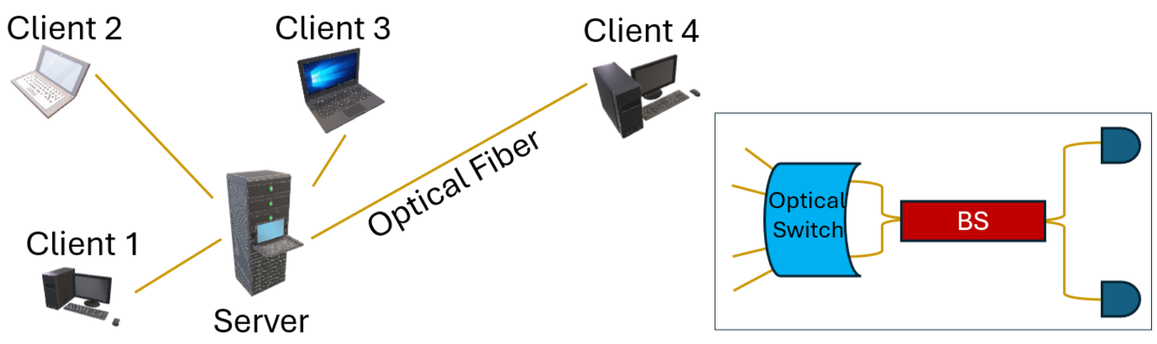

Fig. 1. Schematic of multi-user scheme.

Side-channel attacks on detectors are common, but with the introduction of MDI-QKD, this vulnerability has been addressed. Nevertheless, in practice, multi-user asymmetric channels are often used (figure 1). To effectively enhance the key rate, the 7 intensity protocol has been introduced.

7 intensity Protocol

Step1: Alice & Bob prepare phase randomized weak coherent pulses (WCPs).

Step2: Alice & Bob choose the basis (Z or X), bits (0 or 1), amplitude (s, μ, ν, ω) and send their bits string to Charlie.

Step3: Charlie executes the Bell state measurement (BSM) and announces the successful BSM to Alice & Bob.

Step4: Alice flips or doesn't flip her bits based on the BSM result and basis choice to share secure keys with Bob.

State Preparation

The intensity waveforms to be separately transmitted by Alice & Bob are depicted in Figure 2. $S_A, S_B, \mu_A, \mu_B, \nu_A, \nu_B, \omega$ represent different average photon numbers. We define bit 0 (expressed as $|0\rangle$) & 1 (expressed as $|1\rangle$) in the Z basis. Additionally, we define bit 0 (expressed as $|0\rangle + |1\rangle$) & 1 (expressed as $|0\rangle - |1\rangle$) in the X basis.

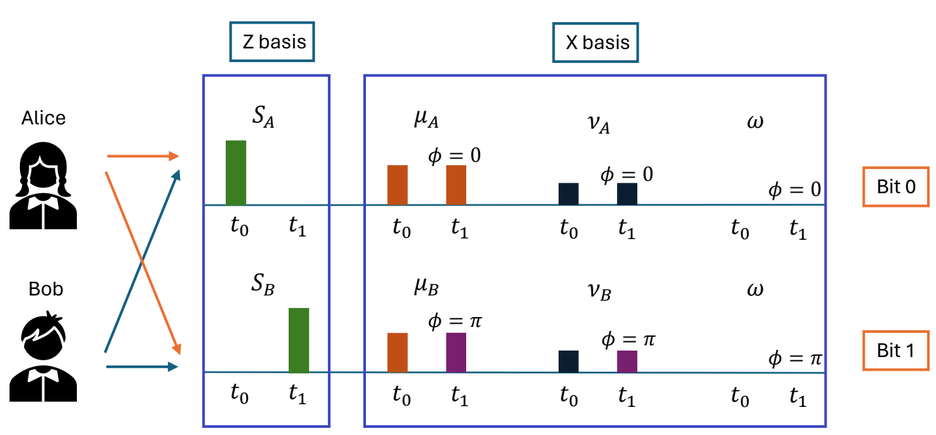

Fig. 2. The states prepared by Alice & Bob.

Sifting

After announcing the BSM results, bit flips need to be performed (Table 1).

Alice & Bob	Relay output $\|\psi^-\rangle$	Relay output $\|\psi^+\rangle$
Z basis	Bit flip	Bit flip
X basis	Bit flip	-

Tab. 1. Sifting process

Experimental Setup

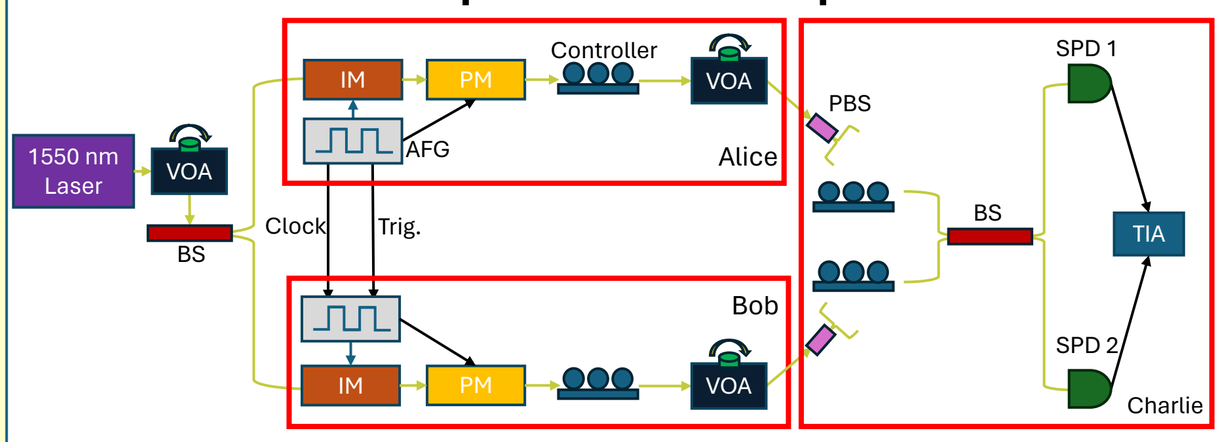

Fig. 3. 7 intensity protocol experimental setup

The setup of our experiment is depicted in Figure 3. A 1550nm laser is directed towards Alice and Bob. The bit information is encoded using the intensity modulation (IM) and phase modulation (PM). After the modulation, we use a variable optical attenuator (VOA) to adjust the light intensity and produce WCPs. Subsequently, the light reaches Charlie, undergoes interference at a beam splitter (BS), and undergoes BSM.

Result

Our current experimental key rate is 17.2 bps. Although this is not the optimal key rate, it represents a 148-fold increase compared to our previous experiments. Detailed experimental parameters are provided in Table 2.

The measured and computed values	Current Data	Previous Data
$Q^z_{\mu\mu}$	232087	376
$Pz * Q^z_{11} * Y^z_{11}$	156163.679 (Pz= 0.25)	342.810 (Pz=1)
e^X_{11}	0.0895	0.143
E^Z_{ss}	0.00880	0.00797
Secret Key Length	68897	110
Measuring Time	4000 s	952 s
Secret Key rate	17.224 bps	0.116 bps

Tab. 2. Experimental data.

148 times higher

Future Work

We plan to test the quantum communication over asymmetric channels between the Physics Building and General Building II (Figure 4). Additionally, we aim to further enhance the key rate using an arbitrary waveform generator to maximize the protocol's potential and surpass the existing instrumentation limitations.

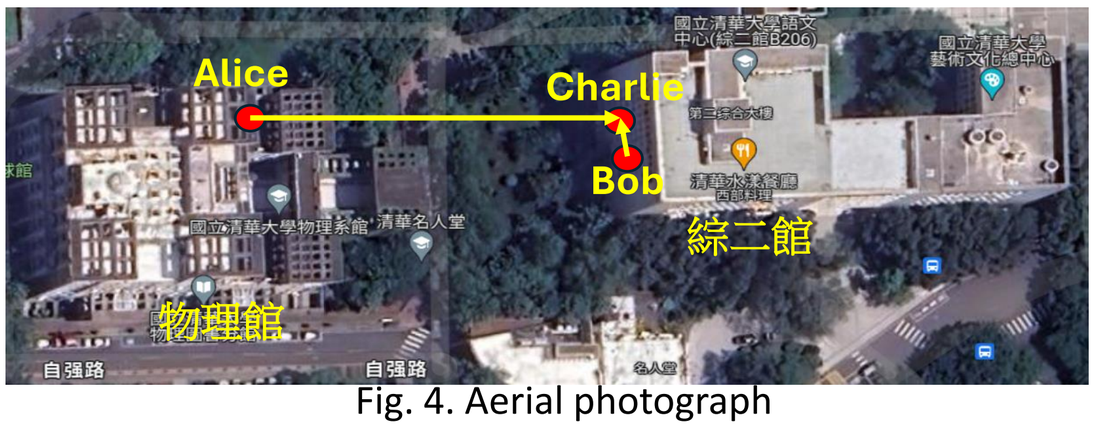

Fig. 4. Aerial photograph

Reference

1. H. K. Lo, M. Curty, and B. Qi, Phys. Rev. Lett., 108, 130503 (2012).
2. H. K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett., 94, 230504 (2005).
3. F. Xu, H. Xu, and H. K. Lo, Phys. Rev. A, 89, 052333 (2014).