

finite detection efficiency. This flaw can allow Eve to perform an *intercept and resend* attack, in which Eve intercepts and measures the state being transmitted and prepares a fake state to be sent to Bob. A MDIQKD network attempts to close the *detection loophole* by **removing the measurement devices entirely** and instead uses a shared central station to create entanglement-like correlations between Alice and Bob through a *Bell-state measurements*(BSM). This approach is based of *time-reversed entanglement based QKD*[2] and **relies on the monogamous nature of entanglement. As Alice and Bob are connected by a fully entangled state, even if Eve completely controls the central station she can not gain any information about the cryptographic key.**

Upgrading a standard QKD network to a MDIQKD network has not been attempted until now as there are two main technical challenges that arise. The first being *reference frame calibration*. This refers the the real time alignment of reference frames between network users. In past attempts to achieve *reference frame calibration* researcher have used additional fibre links between users. The results of this is that the demand of fibre links increases quadratically with the number of network users. This is impractical when scaling up to a city sized user populations. A solution was found by the researchers in China through a *phase feedback scheme*, shown in figure 1. This allowed for a far more manageable linear scaling of fibre links with the number of network users.

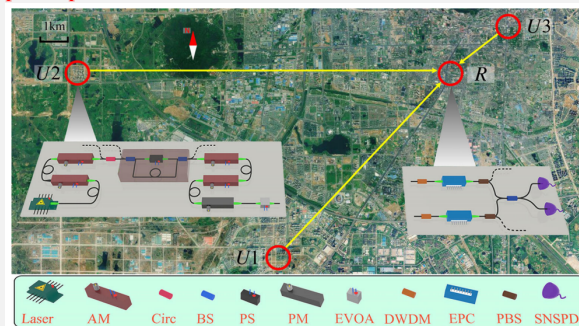
The second technical challenge involves *maintaining indistinguishability* between the network users. In a MDIQKD network any two users can be switched upon request. **The new user's laser must be calibrated immediately to disallow the new and old users lasers from mixing. Mixing two users lasers would result in the timing, spectrum and polarization mode being indistinguishable between the two users.** A solution was developed using *multi-user HOM interference* technology. The team believes this technology can find applications in *multi-party entanglement swapping-based quantum communication* and a *quantum computing cloud*.

Secure key rate 10 times larger than previous results

QKD networks can be characterised by their *secure key rate*. The secure key rate gives a measure of how much secure information (measured in bits) is transmitted per second by the network. It is calculated from the networks gain rates, error rates and error correction efficiency. The secure key rate is distinct from the *key rate* which only gives a measure of how much information is transmitted per second by the network. Compared to standard QKD networks the key rate for an MDIQKD network is relativity low. Under the same experimental parameters a decoy *BB84* system with a trustful relay can generate a key rate around 1000bps, **over 25 times greater than the team achieved in the MDIQKD network.** However, what a MDIQKD network lacks in key rate it makes up with security. Hence, the secure key rate achieved by the team are at least 10 times higher than previous state of the art field tests. The results are shown in figure 2.

Typical MDIQKD Process

1. Alice and Bob both prepare **phase randomized weak coherent pulses (WCPs) in the four possible polarization states ($0^\circ, 45^\circ, 90^\circ, 135^\circ$).**
2. Alice and Bob both send their states to the central relay.
3. **The central relay performs a bell state measurement that projects the incoming signals into a bell state.**
4. The relay publicly announces the bell state.
5. Alice and Bob then publicly announce there basis but not there associated bits.
6. **From the relays bell state, Alice/Bobs basis and knowing there own bit that was sent. Alice/Bob can work out the opposite parties bit that was sent**[4].



5 AT LEAST 3 INTERVIEWS WITH UCL ACADEMICS STATING THEIR VIEWS ON THE PROPOSAL

6 NEXT STEPS IN THIS RESEARCH AREA AND LIKELY TIME-SCALES

REFERENCES

- [1] E. O. Kiktenko, N. O. Pozhar, A. V. Duplinskiy, A. A. Kanapin, A. S. Sokolov, S. S. Vorobey, A. V. Miller, V. E. Ustimchik, M. N. Anufriev, and A. S. Trushechkin. Demonstration of a quantum key distribution network in urban fibre-optic communication lines. *Quantum Electronics*, 47(9):798–802, Sep 2017.
- [2] Eli Biham, Bruno Huttner, and Tal Mor. Quantum cryptographic network based on quantum memories. *Phys. Rev. A*, 54:2651–2658, Oct 1996.
- [3] Yan-Lin Tang, Hua-Lei Yin, Qi Zhao, Hui Liu, Xiang-Xiang Sun, Ming-Qi Huang, Wei-Jun Zhang, Si-Jing Chen, Lu Zhang, Li-Xing You, Zhen Wang, Yang Liu, Chao-Yang Lu, Xiao Jiang, Xiongfeng Ma, Qiang Zhang, Teng-Yun Chen, and Jian-Wei Pan. Measurement-device-independent quantum key distribution over untrusted metropolitan network. *Phys. Rev. X*, 6:011024, Mar 2016.
- [4] Hitoshi Inamori. Security of practical time-reversed epr quantum key distribution. *Algorithmica*, 34:340–365, 12 2002.

4 2 OR 3 "BOXES" EXPLAINING, VIA DIAGRAMS, THE KEY TECHNICAL IDEAS OF THE EXPERIMENT ITSELF OF THE THEORY BEHIND IT