A non-technical explanation of the main achievement of the paper

Nomenclature

BSM	Bell State Measurement
HOM	Hong-Ou-Mandel
$MDIQKD$	Measurement-Device-Independent Quantum Key Distribution
QKD	Quantum Key Distribution

Demonstrating a measurement-device-independent quantum key distribution (MDIQKD) network

Researchers from china have successfully demonstrated a three user, four node *measurement-device-independent quantum key distribution* (MDIQKD) network within the city of Hefei. Previous demonstrations of a *quantum key distribution* (QKD) networks, such as by the team at moscow state university[1] , have been proven to be successful but are vulnerable to attack by an eavesdropper (Eve). Standard QKD networks (also known as prepare and measure QKD networks) have to assume the central relays to be completely trustful. In reality this is extremely unlikely due various security loopholes associated with standard QKD networks. One such security loophole is the *detection loophole*. The *detection loophole* is caused by unavoidable losses in the quantum channel and the coupling between photon source and optical fibres. Additionally losses occur due to the measurement devices 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*. It is calculated from the networks gain rates, error rates and error correction efficiency.

2 or 3 boxes explaining, via diagrams, the key technical ideas of the experiment itself of the theory behind it

Box

...

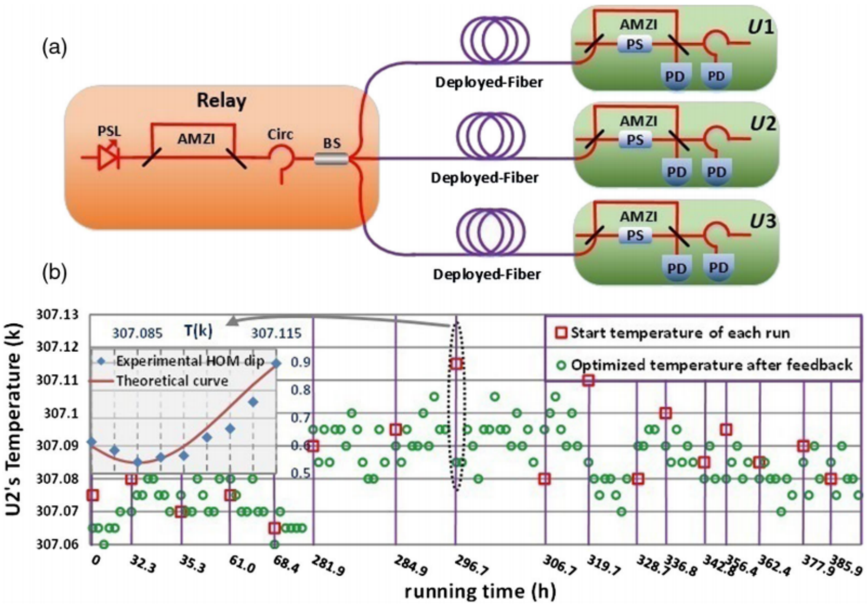

Figure 1: Phase feedback scheme.

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.