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

### Nomenclature

$BSM$ Bell State Measurement
$MDIQKD$ 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.

**Secure key rate 10 times larger than previous results**

...

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

**Box 1**

...

**Box 2**

...

## 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.