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

Nomenclature

$BB84$	Bennett Brassard 1984
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 achieved but are vulnerable to an 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]. The bell state measurement provides a vital piece of information that when combined with the outgoing information, it allows the network users to work out what information is being sent to them. As only the network user knows his/her outgoing information, even if Eve completely controls the central station she can not gain any information about the cryptographic key. For a MDIQKD network to be successful it requires that the network users have almost perfect state preparation (fully know what their outgoing information is). However this issue is easily addressed as their states can be experimentally verified in a fully protected laboratory environment, outside of Eve's interference.

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.

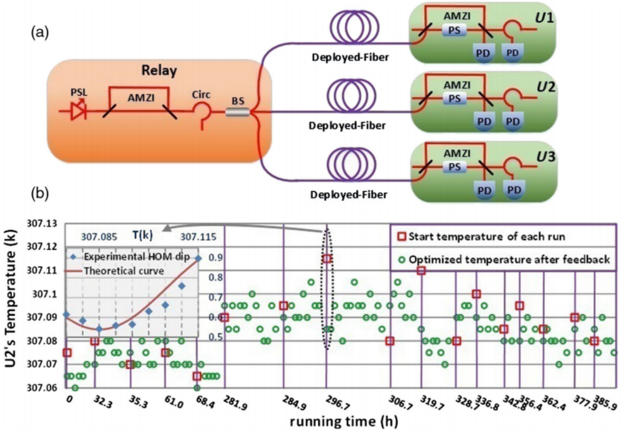
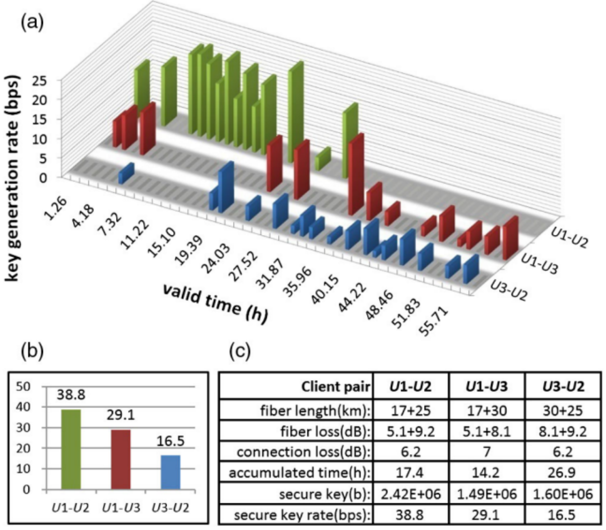


Figure 1: Phase feedback scheme[3].



Client pair	U1-U2	U1-U3	U3-U2
fiber length(km):	17+25	17+30	30+25
fiber loss(dB):	5.1+9.2	5.1+8.1	8.1+9.2
connection loss(dB):	6.2	7	6.2
accumulated time(h):	17.4	14.2	26.9
secure key(b):	2.42E+06	1.49E+06	1.60E+06
secure key rate(bps):	38.8	29.1	16.5

Figure 2: Secure key rate.[3].

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

A Typical MDIQKD Process

1. Alice and Bob both prepare outgoing signals in the four possible polarization states $(0°, 45°, 90°, 135°)$.
2. Alice and Bob both send their states to the central relay via optical fibres.
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 outgoing bit. Alice/Bob can work out the opposite parties bit that was sent.
7. Process is repeated until cryptographic key is built up.

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 untrustful 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.