Measurement Device Independent Quantum Key Distribution Network

Chris Irish and Jonathan Gough

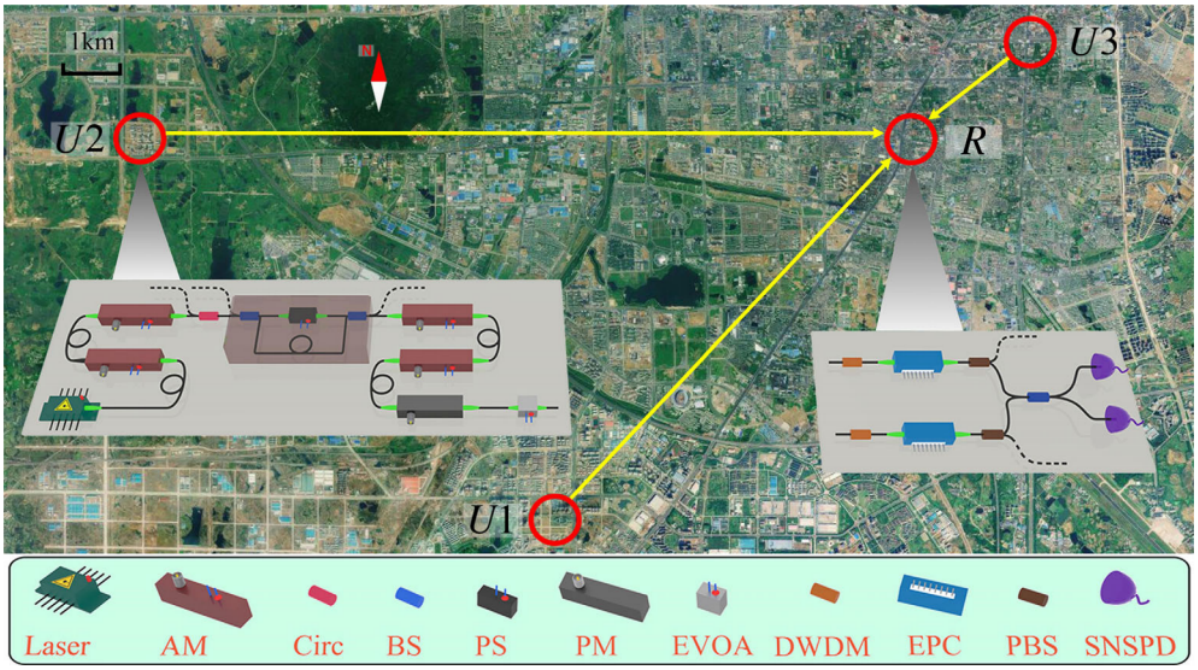

Fig. 1. Birds-eye view of the MDIQKD network topology[3].

Abstract— With the every advancing development of quantum computation and its ability to breech current security protocols, new approaches to quantum cryptography must be developed. One such approach is *Measurement Device Independent Quantum Key Distribution*. Up until now, MDIQKD has been largely theoretical. For the first MDIQKD has been experimentally verified by researchers from China. A three user, four node MDIQKD network was achieved within the city of Hefei. A **”step in the right direction towards a secure global network”** says one leading MDIQKD theorist.

Index Terms—MDIQKD, QKD, BB84

1 Quantum Cryptography

At the heart of private communication measures is the establishment and distribution of encryption keys secretly and securely. While the prodigious prime factorisation abilities of quantum computers seem set to make a mockery of our best existing cyber-security measures, study of quantum communications has simultaneously unearthed a possible lifeline, in the form of a new secure key method, whose integrity against eavesdroppers comes with a cast iron guarantee, backed by the laws of quantum physics. At least in theory. Meet Eve, the cardboard eavesdropper. She lurks in every theoretical communication model, able to instantly recognise any potential weakness, able to call on any and all existing resources to aid in its exploitation. A ruthless predator on a single-minded hunt for illicit data, intent on maximum personal damage to Alice and Bob, our humble network users, she won’t rest until maximum ruination is achieved.

Manuscript received 21. 06. 2019; accepted 21. 06. 2019. Date of Publication 21. 06. 2019; date of current version 21. 06. 2019. For information on obtaining reprints of this article, please send e-mail to: jonathan.gough.18@ucl.ac.uk.
Digital Object Identifier: xx.xxxx/TVCG.201x.xxxxxxx/

2 Enter Quantum Key Distribution

The Quantum key distribution (QKD) network provides a possible solution. Assuming she can find out the bases being used, Eve may then try to intercept Alice’s photon, preparing a fake state to send on to Bob, which is known as an intercept and resend attack. However, as long as Alice and Bob keep their basis choices secure during the process, Eve has no way to find them out, and subsequently can never be certain of the original value of the bit.

The best she can do is pick randomly, and send her measured state on to Bob. On top of her 50$rightbasis, ifshepickswrong, shestillhasa$50to guess the right value, meaning shell only be wrong a quarter of the time, but it turns out that will be enough.

Afterwards, Alice and Bob share the sequence of bases they used over the phone. Eve has, of course, bugged the line and hears everything, unbeknownst to our duo.

Alice and Bob discard all the results where they used different bases (roughly half), and sacrifice a section of the remaining code by confirming it over the insecure line. By analysing the compromised results, the unavoidable error rate introduced by Eves tampering, is increasingly easily identified, the more photons she pilfers.

However, all is not lost for Eve, as its a long walk from chalkboard to lab, and she has far sneakier means at her disposal. The real world introduces various problems such as environmental and atmospheric interference, inherent device inaccuracies, creeping alignment errors, and other physical limits to accuracy and scope. And sure enough, down amongst the decay, in with the interference, is Eve, trying to mask her activity behind the systemic noise.

QKD BASICS

We can create, and transmit, photons with chosen qubit states encoded into their polarisation direction. A vertically polarised photon, or $\uparrow$, corresponds to a 0 in our data, while horizontal polarisation, or $\rightarrow$, corresponds to a 1. If we align the emitter with the detector, then when a photon prepared as $\uparrow$, or 0, for instance, reaches the detector, it is measured as $\uparrow$, or 0, with certainty.
More interestingly, when we tilt either our emitter, or our detector, relative to the other, the probabilities are shifted smoothly from one outcome towards the other. Our measurement will still either be $\uparrow$ or $\rightarrow$ with overall certainty, but with a chance of each outcome. If we tilt our devices at 45° to each other, a photon prepared in either state, $\uparrow$ or $\rightarrow$, will be measured as $\uparrow$ or $\rightarrow$ with 50/50 chance, and the original information is lost. BB84 is a common protocol, which uses two different bases, ($\uparrow$, $\rightarrow$) and ($\nwarrow$, $\nearrow$), that are at a 45° angle, and employs random number generators to randomise basis choice for both devices, as well as the choice of bit. Interference by Eve can be detected by analysing discrepancies in Alice and Bob's results.

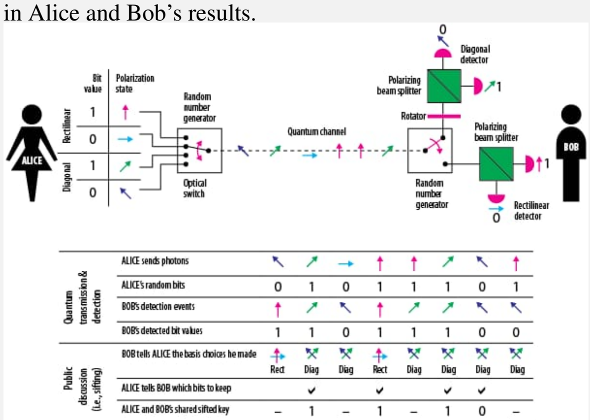

Image source: UNS Nice (France), Department of Physics.

3 THE LIMITS OF QKD

"There is no thing as security if it always requires some assumptions". Dr Lluis Masanes, A leading researcher on quantum information sciences at UCL has his doubts on standard QKD network security.

Previous demonstrations of a *quantum key distribution* networks, such as by the team at Moscow State University[1] , have been achieved but are still vulnerable to an attack by 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 these 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 attack such as an *intercept and resend*.

4 THE FUTURE OF QKD

A MDIQKD network attempts to close the *detection loophole* by removing the standard measurement devices entirely and instead uses a shared central station to create entanglement-like correlations between Alice and Bob through *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 an 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.

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 network's 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 for with security. Hence, the secure key rate achieved by the team is at least 10 times higher than previous state of the art field tests.

Prof Alessio Serafini, professor of theoretical physics at UCL reinforced the importance of the team's work for the field of quantum information.

" The theory becomes true when you build a machine with it and Device Independence is very instrumental to this because it tells you these machines can only be quantum, that's in the end what it is.".

5 THE LIMITS OF MDI

Upgrading a network from standard QKD to MDIQKD 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* researchers have used additional fibre links between users. The results of this is that the demand for 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 through a *phase feedback scheme*, which allows 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 signals must be calibrated immediately to disallow the new and old user's signals from mixing. Mixing two users signals would result in the timing, spectrum and polarization mode being indistinguishable between the two users. A solution was developed using a technology called *multi-user HOM interference*. The team believes this technology can find applications in *multi-party entanglement swapping-based quantum communication* and *quantum cloud computing* .

Typical MDIQKD Process

1. Alice and Bob both prepare outgoing signals in the four possible polarization states.
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 their bases but not there associated bits.
6. From the relay's bell state, Alice/Bob's bases and knowing their own outgoing bit. Alice/Bob can work out the opposite party's bit that was sent.
7. The process is repeated until cryptographic keys are built up.

Dr Masanes believes fully *Device Independence* in provides, in theory, the most secure approach to QKD

"It is easy to say that it is the most secure framework, but only given that you define the problem in a way that it is possible at all to do it."

He believes the problem is in the implementation, as it seems that security loopholes are unavoidable with physical constraints. "Okay, for instance, if my device also broadcasts my secret key it doesn't matter what you do, it's impossible to achieve absolute security". Alternatives exist that attempt to balance theoretical ambitions and practical constraints, such as Semi-Device Independent QKD, which requires putting complete trust in some of the devices within your network to boost security overall. The advantage of MDI-QKD is that no devices need to be trusted at all. Another issue arises when considering longer distance secure networks as they require additional relays per every few kilometres. "Errors add up in a pretty bad way", says Masanes. Furthermore increasing the number of devices introduces new opportunities for Eve to attack. "What could the adversary do if she had control over the relay? Maybe if she does things cleverly, there is not much that you could do about it".

6 The Future of MDI

Scientists are already looking into solutions to these issues, and one new direction they're looking is upwards. "Satellites should be the next step", says Dr Serafini. "If you are able to get above the dense (atmosphere), to almost free space, the signal is less vulnerable to attack", adds Masanes. There are also further potential benefits, such as the presence of existing global satellite networks that could potentially be integrated into QKD networks, and in terms of reducing device requirements, "well, the satellites are very convenient, because otherwise, when the network is big, you need to build lots of optical fibres, for instance". QKD networks are already used in some specific situations within the private sector, such as in secure business transactions. But will developments such as MDI-QKD ever see use by the general public? Masanes and Serafini agree that they probably will, but differ over the time frame. Serafini predicts public systems in as little as 5-10 years, whereas Masanes is a little more conservative. "In 15 years (it might be possible) just to say something. Yeah, but I don't think that in 15 years our society will have this (quite yet)".

It seems likely that before too long, you might find yourself navigating the quantum network, filling in your quantum tax returns. In any case, it looks like Eve's criminal career may soon be over.

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.