Building blocks for a quantum internet

Joop Hendriks* and Caspar H. van der Wal†
Physics of Quantum and Nanodevices, Zernike Institute for Advanced Materials,
University of Groningen, NL-9747AG Groningen, The Netherlands

(Dated: 22 May 2020)

If one thing has changed our daily lives over the past 20 years, it must be the internet. At the start of the century, you still had to dial-up per phone for internet access. Cat videos were of course unheard of in those days due to slow internet and Youtube did not even exist. But now, more than 98% of the Dutch population has access to the internet [1], almost anywhere and at any time. In times of social distancing and lockdowns for the COVID-19 pandemic, internet bring us together through Skype, Hangouts and Jackbox, still allowing for much needed social interaction. Staying home full-time would for sure have been very different in the pre-internet age.

Much of those enormous streams of data are not meant to be shared, especially not if it concerns your medical information or a bank transfer. That's why data is often encrypted (i.e. transformed by some mathematical operation) when transmitted, so that an eavesdropper cannot make sense of it. The transmitting and receiving parties know which exact mathematical operation was used (they have key), and for as long as they are the only ones who have the key, they can securely send their data. However, there is no proof that the current algorithms are fundamentally secure. If somehow the eavesdropper finds a smart way to greatly increase his computer power (or even finds out how to use a quantum computer) to retrieve the key, he can possibly decipher the information.

How can we keep data transmission secure in the future? Is there a way to even make it fundamentally secure? The answer is yes. By making use of quantum mechanics, quantum key distribution can make it possible. With quantum key distribution, an attempt to eavesdrop on the key is always detected, in which case the actual message will not be sent before distributing a new key and the information is kept safe. In case you are interested and want some background information, there are some nice earlier publications from our group [4–6]. For distributing quantum keys, you need to send quantum information from one end to the other. In more general terms, as you want to be able to do this with many different possible connections, you need a quantum internet! The most popular carriers for sending quantum information around this internet are few-photon pulses, as they can travel fast over large distances if they are guided in optical fibers. But even for the best fibers, the attenuation (photon-loss) length is on the order of 100 km, by far not enough if you want to send information across the ocean. The solution to this is to place quantum repeater boxes at fixed distances in the communication channel.

But repeating (as in current internet repeaters) a quantum state is tricky, as measuring such a state will immediately disturb the state of the photonic pulse (this is of course exactly why one cannot eavesdrop). A protocol called the DLCZ protocol describes how these boxes can be used to achieve communication over large distances by making use of atomic ensemble (i.e. a lot of individual atoms) and photons in a clever way [2].

The goal of the DLCZ protocol is to *entangle* two ensembles at the far ends of the communication channel. How we can get there and what it means is schematically illustrated in Figure 2. There are two atomic ensembles, I and

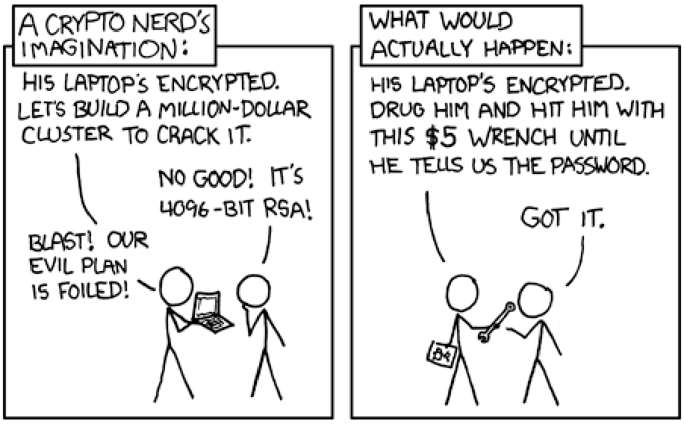

FIG. 1: Information is only fundamentally secure in an information-theoretical sense [7].

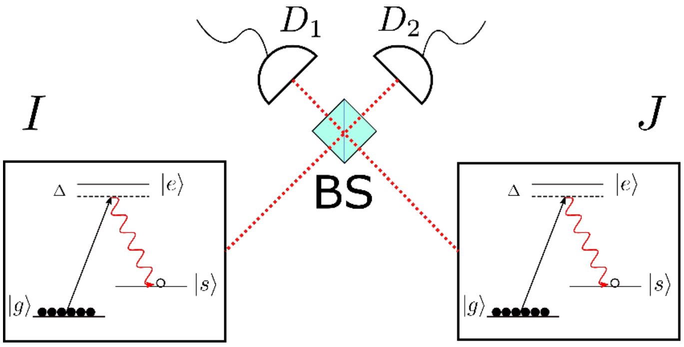

FIG. 2: Entanglement between two ensembles. Ensembles I and J are both illuminated with a weak laser, detuned by an energy Δ, such that on average less than one photon is emitted from either ensemble. The emitted photon pulses are combined in a beam splitter BS. Upon detection of a single photon in detectors D_1 or D_2, the two ensembles are in an entangled state. Figure adapted from [3].

J, with three relevant energy levels as drawn inside the squares representing the ensembles. In a simplified picture, we can assume that all atoms in the ensemble have the same three level energy structure where a single electron can occupy one of the levels, so we can prepare the ensembles such that the electrons from all atoms are in state $|g\rangle$. The next step is to excite the ensembles to state $|e\rangle$ with a short laser pulse such that on average less than one photon is emitted from a subsequent $|e\rangle$-$|s\rangle$ transition, from either of the ensembles. We ensure that this requirement is fulfilled by using a sufficiently weak laser beam which is also slightly detuned, i.e. the driving laser photon energy is lower than the energy difference $|e\rangle$-$|g\rangle$ by an amount Δ. This can lead to the emission of a photon with a frequency that is lower than the laser frequency by the energy difference between $|g\rangle$ and $|s\rangle$. Next, the output pulses of both ensembles are filtered from the laser pulse and combined in a 50/50 beam splitter, where two single-photon detectors are positioned at the two output channels. If one of the detectors counts a photon (click!), you know that one ensemble contains a single excitation at level $|s\rangle$, but the beam splitter removed all information about from which of the ensembles it came from. This means the systems are now in a superposition of zero and one excitation, as you fundamentally cannot know where the photon came from. With the mapping $|0\rangle = |g\rangle$ (zero excitations in the ensemble) and $|1\rangle = |s\rangle$ (one excitation in the ensemble), this state can be written as (here we omit a phase factor for simplicity, but also in reality this phase factor can be 1 by carefully tuning your setup):

$$\psi_{IJ} = \frac{1}{\sqrt{2}}(|1_I\rangle\,|0_J\rangle + |0_I\rangle\,|1_J\rangle) \tag{1}$$

This is what is called an entangled state. It means that if you measure that the state of ensemble I is $|0\rangle$, the state of J becomes $|1\rangle$ at that same moment (as in the Einstein-Podolsky-Rosen paradox).

Let's assume that we now want to entangle two ensembles that are separated by several thousands of kilometers. That is by far too long if we want to do that in one go. The photon will be absorbed by the fiber before it reaches the beam splitter. But fortunately, we have enough quantum repeater boxes that we can put at fixed distances so that the communication channel from A to Z is now divided in a number of segments shorter than 100 km. We can do the entanglement trick for all segments first, as shown in Figure 3a. After that's done we can reduce the number of segments by halve by *entanglement swapping*, a process that is very similar to entangling two ensembles. Here, we look at two neighboring segments, each contains two entangled ensembles with a single excitation. In the swapping step, a strong laser pulse, the read pulse, will read out the state in two unentangled ensembles by efficiently converting the excitation to a photon pulse. The pulses are combined in a 50/50 beam splitter, and upon measuring one photon, we know there is still one excitation left in the system but due to the beam splitter it is again impossible to know where and the previously unentangled segments are now entangled (Figure 3b). If you repeat the swapping operation step until there is only one very long entangled segment left, you have successfully entangled the qubits at A and Z (Figure 3c).

But there is a caveat: entangling two qubits is a probabilistic process, since it depends on detecting a single photon at one of the detectors while the probability of emitting a single photon must be smaller than one. If there are no photons detected, it means that the entanglement operation did not succeed. Now there are two options: you can either try to entangle all segments until by chance they are all successfully entangled successfully at the same time,

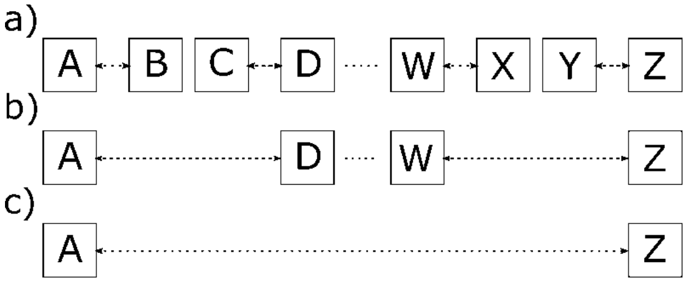

FIG. 3: a) Entanglement over a large distance can be achieved by first entangling a number of short segments. The arrows indicate an entangled segment. b) after the first swapping step, the distance over which two ensembles are entangled doubles. c) The swapping step needs to be repeated until the ensembles at the far ends are entangled directly. Figure adapted from [3].

or you try to store the entangled states and retry to the entangle the segments that weren't successful in the previous trial. The first option might work for a short distance but becomes very inefficient for longer distances. The second option is much better in that regard, but means that the ensembles must be able to keep the entangled state they're in stable for some time, i.e. they must serve as a quantum memory!

In the Physics of Quantum Devices group we are working, together with a European consortium of eight other research groups, on the realization of a quantum memory. In this project, called QuanTELCO [8], we are using silicon carbide (SiC) with transition metal impurities. SiC is a material which is widely used in the semiconductor industry, mature fabrication processes are readily available and a lot is already known about the optical and electronic properties of SiC with transition metal impurities. For this project, we are specifically interested in SiC with vanadium impurities, since these defects can absorb and generate single photons around 1300 nm. This wavelength is particularly interesting because it is right in the middle of the telecom O-band (1260-1360 nm), a range where the attenuation of the optical fiber very low and which makes it compatible with the current telecom technology and existing optical-fiber networks. This is also what makes this material unique, as competing materials do not directly emit at this wavelength and require tricks like frequency conversion before the photonic pulses can be sent across large distances.

However, many basic properties of vanadium defects in SiC are still unknown. In the coming years, we will study the physics of this interesting material and hopefully find answers on questions like: how do electron spins in the ensemble couple to photons? Why are the spin excitations disturbed by phonons and what are the processes behind it? Answers that will help us to better understand this material, which is much needed before a we can prepare a successful demonstration of a working SiC-based quantum memory and bring us one step closer to fundamentally safe communication.

References

---

[*] Electronic address: `j.hendriks@rug.nl`
[†] Electronic address: `c.h.van.der.wal@rug.nl`

[1] https://www.cbs.nl/nl-nl/nieuws/2018/05/nederland-koploper-in-europa-met-internettoegang

[2] Long-distance quantum communication with atomic ensembles and linear optics. Duan, L. M., Lukin, M. D., Cirac, J. I., and Zoller, P., Nature, 414, 413 (2001; https://doi.org/10.1038/35106500

[3] Quantum repeaters based on atomic ensembles and linear optics. Sangouard, N., Simon, C., De Riedmatten, H., and Gisin, N., Reviews of Modern Physics, 83, 33 (2011); https://doi.org/10.1103/RevModPhys.83.33

[4] Securing communication with quantum physics. Caspar van der Wal, Periodiek 4 (University of Groningen, 2011); available at http://www.quantumdevices.nl/publications/

[5] Controlling spins and photons for fundamentally secure communication. Caspar van der Wal, Lustrum book 2009-2014, p. 102, Applied Physics student society Professor Francken (University of Groningen, Oct. 2014); available at http://www.quantumdevices.nl/publications/

[6] Veilig communiceren met quantummechanica. Caspar van der Wal, Nederlands Tijdschrift voor Natuurkunde 80, 186 (June 2014); available at http://www.quantumdevices.nl/publications/

[7] Source: https://xkcd.com/538/

[8] QuanTELCO websites: https://quantelco.univie.ac.at/ ; https://cordis.europa.eu/project/rcn/224946/en