Controlling spins and photons

For fundamentally secure communication

Prof. dr. ir. C.H. van der Wal

The science and techniques for securing long-distance communication against eavesdropping are known as cryptography. While this used to be associated with spies and war activities, several events during the last five years have increased the awareness that it is of interest for almost all groups in our society. The internet is now used for communicating and controlling credit card transactions, personal e-mails, medical records, settings for big power plants, etc. Leaks in the security of such communication systems frequently made the news.

Caspar van der Wal is professor in the group Physics of Quantum Devices. The research of his team focuses on exploring spintronic and quantum information functionalities with electron spins and nuclear spins in semiconductor devices, using both quantum optical methods and electron transport methods.

It is remarkable that there is no mathematical evidence that the methods currently in use for cryptography (such as HTTPS internet traffic) are secure [1]. Research activities in this area therefore look for better methods, and since about 1980 scientists realized that applying the laws of quantum mechanics to information science provides a path to making communication really secure [1, 2, 3]. That is, one can prove that eavesdropping is fundamentally impossible if one assumes that quantum theory is correct. Treating information quantum mechanically means that a signal of one bit of information that is communicated can not only have the value 0 or 1. The bit that is communicated can have any superposition state, $|\Psi_{\text{bit}}\rangle = \alpha|0\rangle + \beta|1\rangle$. α and β are the probability amplitudes for the quantum states $|0\rangle$ and $1\rangle$. The fundamental security comes from the fact that it is impossible to measure or copy the state of such a bit without disturbing it [1].

In practice, the field of quantum cryptography works with the quantum states of optical pulses at the single-photon level that travel in fibers. If a memory function is required [4], the best candidates are the quantum states of nuclear or electronic spins of trapped atoms or ions, or such spins in optically active solids (semiconductors, or transparent crystals with optically active defect sites). However, playing with quantum states is very difficult. If you work with physical realizations that you can control and measure, you suffer from the fact that any noise from the rest of the universe (environment) will also easily disturb the quantum state in an unpredictable manner. If you work with quantum systems that are less sensitive to noise, it also means that they are much harder to control or measure for your application. This shortly summarizes why little devices for quantum cryptography are not yet for sale for 1 nor 100 euro.

Proof of principle demonstrations have been realized in laboratories, but often still require complex and expensive instrumentation, not to mention it often works at 4.2 K and not yet at room temperature. The only exception is a protocol that uses the linear polarization state of single photons (known as the BB84 protocol), that works for distances up to about 100 km on a dedicated fiber, and which has been put on the market by a few companies (see for example [5]).

Improving systems for quantum cryptography is therefore an active re-

[1] For a good recent review and introduction to the field, see: *The ultimate physical limits of privacy*, Artur Ekert and Renato Renner, *Nature* **507**, 443 (2014)

[2] *The quantum internet*, H. J. Kimble, *Nature* **453**, 1023 (2008).

[3] *Privacy and the Quantum Internet*, Seth Lloyd, *Scientific American*, p. 80 (Oct. 2009)

[4] *Long-distance quantum-communication with atomic ensembles and linear optics*, L.-M. Duan, M. D. Lukin, J. I. Cirac, P. Zoller, *Nature* **414**, 413 (2001)

[5] http://www.idquantique.com/ and http://swissquantum.idquantique.com/?Key-Sifting

search field, with steady progress both conceptually for better protocols [1] as well as for the physics and materials science for the realization of practical systems. In the remainder of this article I will introduce some fundamentals of the current research activities on quantum cryptography of my team, which aims at exploring suitable material systems. In addition, I will discuss one amazing breakthrough of others in the field. For the basics of how and why quantum protocols are secure, I refer the reader to two related articles that I recently wrote for a similar audience as this article: the principles of the BB84 protocol (which uses quantum superposition states of the polarization of single photons) were summarized in [6]; protocols that use optical pulses that are a superposition of 0 and 1 photon were summarized in [7].

The breakthrough that was published in 2013 concerned an experiment where spin states could be preserved for half an hour at room temperature.

In the field that aims to get better memory functions on the quantum states of spins in solids, the year 2013 showed a remarkable breakthrough. To appreciate this, I should mention that over the last 20 years research activities already aimed at keeping spin states $\Psi_{\text{spin}} = \alpha \left|\uparrow\right\rangle + \beta \left|\downarrow\right\rangle$ undisturbed for a long time. However, physicists were typically struggling to keep the state pure for timescales longer than microseconds (at least for materials and structures that seemed to have some relevance for real devices). Note that this timescale has relevance with respect to the timescale that is needed for an optical pulse to travel between two distant points on our planet, say the distance from Groningen to New York (a distance of about $L = 6000\,\text{km}$). Thus, such memory functions can do something useful if the quantum state can be preserved for at least a time $L/c \approx 20\,\text{ms}$ (c is the speed of light) [4,7]. The breakthrough that was published in 2013 concerned an experiment where spin states could be preserved for half an hour at room temperature [8].

What was needed to accomplish this? The research team managed to put their spins in the something they called the *semiconductor vacuum*. This is not a vacuum at all, but a big single crystal of

[6] *Securing communication with quantum physics*, Caspar van der Wal, *Periodiek* **4**, 2011; available on http://www.quantumdevices.nl/publications/

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

[8] *Room-Temperature Quantum Bit Storage Exceeding 39 Minutes Using Ionized Donors in Silicon-28*, K. Saeedi *et al.*, *Science* **342**, 830 (2013)

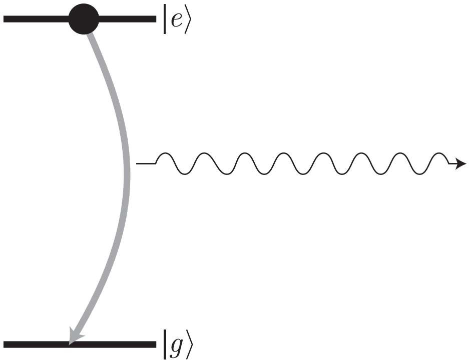

Figure 1. When an atom is in its exited state $|e\rangle$ and it relaxes to the ground state $|g\rangle$ it will emit exactly one photon.

silicon. For preserving quantum states of spins it was indeed the best empty environment that has ever been realized. If you want to preserve the quantum state of the spin of a single atom in an empty (that is, low-noise) environment, you must use some container and pump it as close to vacuum as possible. There are limitations on how low you can make the pressure. Thus, you will always have collisions between your functional atom and other, unwanted, atoms. In addition, your functional atom should not float away, so you must allow for electromagnetic fields that can be used for trapping the atom at some location, and thereby you also open the door for noise reaching the atom.

The work on the single crystal of silicon used the spins of isolated donor atoms (phosphor atoms) in the lattice of silicon. The spins used were the nuclear spin of these donor atoms. To remove noise sources, the donor electrons were removed. Also, it required that the silicon lattice only consisted of silicon atoms with zero nuclear spin. This is not the case for the silicon that you get when you use what nature provides. Natural silicon consists three isotopes: 95% ^{28}Si and ^{30}Si (with nuclear spin 0) and about 5% ^{29}Si (with nuclear spin $I = 1/2$). This research used silicon that was isotopically purified (almost pure ^{28}Si). Regrettably, this is not commonly available. On this occasion, it was a side product of another big scale research effort: making a near-perfect sphere of pure ^{28}Si as a path to a better and reproducible definition of the SI standard kilogram [9].

My team studies the electronic spins of materials where the spin states can potentially be preserved for more than 20 ms, but where the optical properties are much better than for silicon and where the fabrication costs of devices can be low. Our experiments really test the most basic functionalities that are needed, and these can be summarized as follows:

1. Produce an optical pulse that is a superposition of 0 and 1 photon. As discussed below, you can in fact only do this if the light-emitting quantum system is in a quantum superposition of two spin states after the emission.
2. Collect the emitted optical pulse with high efficiency.

So, let's consider the task to create an optical pulse that is a superposition of 0 and 1 photon. How can you do this?

[9] http://phys.org/news/2011-02-kilogram-approaching-avogadro-constant-enriched.html

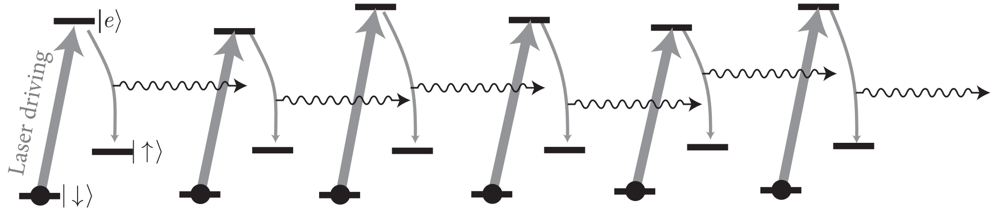

Figure 2. Ensembles of three-level systems that have an excited state $|e\rangle$, and two low-energy states that are spins states $|\uparrow\rangle$ and $|\downarrow\rangle$.

To get on the right path, consider a single atom (with one electron in its outer shell) that is in its excited state $|e\rangle$. If this atom relaxes to the ground state $|g\rangle$ it will emit exactly one photon, as illustrated in Figure 1.

So if you can prepare this system to be initially in state $|e\rangle$, and then control it to relax to a quantum superposition state of $|g\rangle$ and $|e\rangle$, this process goes along with the emission of an optical pulse that is a superposition of 0 and 1 photon (for this we will introduce the notation $|0_{\text{phot}}\rangle$ (no pulse) and $|1_{\text{phot}}\rangle$ (a pulse of a single photon)). Note, however, that there must then be correlations between the quantum states of the atom and the optical pulse. In fact, you are only allowed to write the quantum state (the superposition of states) in this form: $|\Psi\rangle = \alpha|e\rangle|0_{\text{phot}}\rangle + \beta|g\rangle|1_{\text{phot}}\rangle$. The atom and optical pulse together form one quantum system, you can no longer properly describe the quantum state of one part on itself. This phenomenon is known as entanglement between the state of the atom and the pulse (you may have heard about *entanglement* from its role in the Einstein-Podolsky-Rosen paradox). Interestingly, you can look at this as if the superposition of the states $|g\rangle$ and $|e\rangle$ is a memory of the state that is carried away by the optical pulse, and this is in fact a powerful ingredient for the quantum cryptography protocols[4].

In practice, you cannot do it as derived in the previous paragraph because it is nearly impossible to have any control over the spontaneous optical emission that happens when the system relaxes from $|e\rangle$ to $|g\rangle$. In addition, for such a single atom the emitted light will really go in all directions, and in practice this means that it is very difficult to detect the emitted light with an efficiency of more than 0.1% (unless you do some very difficult engineering and place the atom exactly between two near-perfect mirrors in an optical cavity). In our work, we therefore work with *ensembles* of three-level systems, as in Figure 2.

These three-level systems have an excited state $|e\rangle$, and two low-energy states that are spins states $|\uparrow\rangle$ and $|\downarrow\rangle$. In our labs we work with basic semiconducting materials, and the spin is the electronic spin of a localized donor electron in GaAs, or that of a lattice-vacancy defect in SiC.

With this ensemble approach with

a three-level system many things work better, and in a manner that is also robust against technical imperfections that you always have in practice. In order to control the emission of an optical pulse, the systems are first prepared in the state $|{\downarrow}\rangle$ (using lasers that pump the electron in that state for each system). Next, if a laser pulse is resonantly driving the $|{\downarrow}\rangle$–$|e\rangle$ transition, then and only then the systems will get excited and have the opportunity to spontaneously emit some light from making a $|e\rangle$–$|{\uparrow}\rangle$ transition. Thus, if you make the laser driving weaker or shorter, you can control the full ensemble to only emit a tiny amount of light from the $|e\rangle$–$|{\uparrow}\rangle$ transition, that is in fact a superposition of 0 and 1 photon (the emission per three-level system is then indeed only a fraction of that). If you place all the three-level systems on a row, you profit from the effect that almost all of the emission goes along the row, and this allows for detecting the emitted light with near 100% efficiency in a robust manner. The reason is that the initial emission of the $|e\rangle$–$|{\uparrow}\rangle$ transition will still go in all directions, but the component that travels along the ensemble will grow much faster (get amplified) via the principles of stimulated emission. In practice this is compatible with an elegant engineering approach: we simply build one-dimensional waveguides (short pieces of optical fiber) of the material that contains the three-level quantum emitters.

A further advantage is that the state after emission (memory function) is a superposition of the states $|{\downarrow}\rangle$ and $|{\uparrow}\rangle$, and these live much longer than a superposition of $|g\rangle$ and $|e\rangle$ from the two-level atom example. Finally, you may notice in the figure that the energy distance between the states $|{\uparrow}\rangle$ and $|e\rangle$ is not the same for each system, while it is the same for the states $|{\downarrow}\rangle$ and $|{\uparrow}\rangle$. This corresponds with the situation in practice that small amounts of strain in materials cause shifts in the $|{\uparrow}\rangle$–$|e\rangle$ energy difference, but almost don't for the spin splitting. In our three-level system approach (see figure) the photon energy of the emitted light for each system is that that of the driving laser minus the $|{\downarrow}\rangle$–$|{\uparrow}\rangle$ energy splitting, and thereby insensitive to the inhomogeneity of the $|{\uparrow}\rangle$–$|e\rangle$ splitting. This is in practice essential for getting sufficiently precise control over the photon energy of the emitted light.

In summary, quantum cryptography can bring communication for which eavesdropping is impossible. For getting such systems on the market, the field is still facing some interesting challenges. Quantum physics and material science still provide a wealth of possibilities that we do not yet fully understand and only begin to explore now and which provide an exciting playground for academic research.