# Securing communication

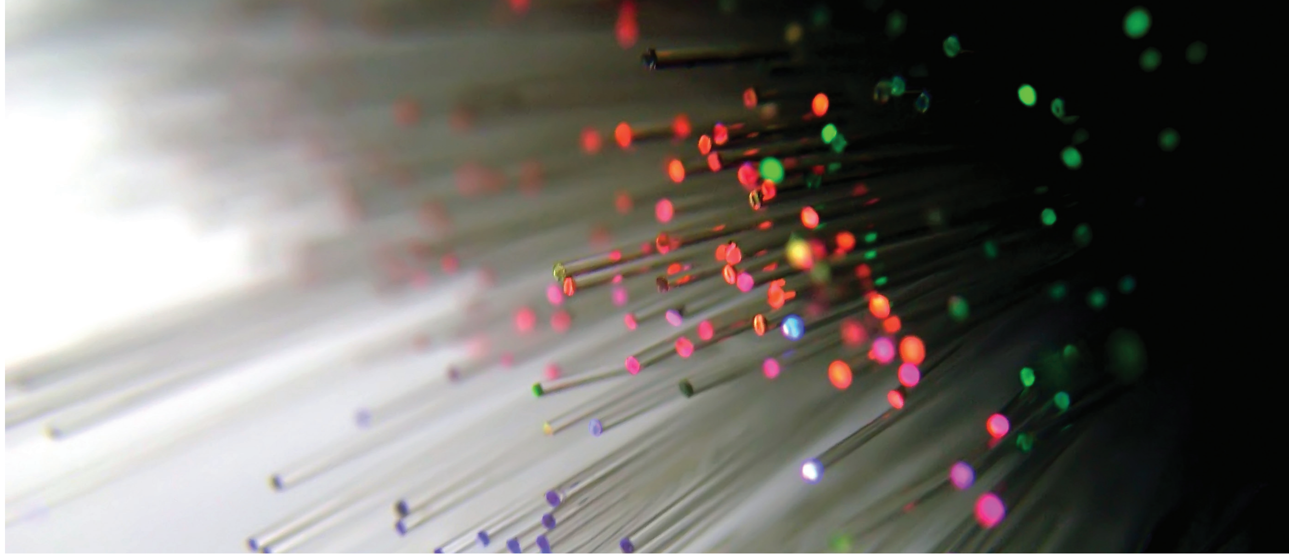
DOOR **CASPAR VAN DER WAL**

In most urban areas, people lock the door when they leave their home. It is simply a reality that this is needed for protecting your privacy and valuable items at a reasonable level against theft. But in our modern lives, much of what is of value can be stolen from us via the internet. We almost constantly use the internet for exchanging personal information, controlling bank and business transactions, and maintaining medical and insurance records. This comes along with possibilities for crime. The need to protect information during such communication against eavesdropping is therefore now just as important as locking the door of your home.

There is, therefore, almost always a form of encryption (also known as cryptography) applied when you use the internet for exchanging information that should remain secret to outsiders. A well-known example is that the connection uses an *https* protocol in instead of a plain *http* protocol. Encryption is making communication incomprehensible to an eavesdropper by applying a mathematical operation to the information (which you can think of as a long row of 1's and 0's in digital representation) before sending it off, and the receiving party knows how to turn this back in the original row of 1's and 0's.

Let's make encryption a bit more vivid with a simple example. Say, it is needed for some reason that you send the PIN code for your bank card to a party you trust. Assume your pin number is 2360. If you and the receiving party both have the same random number in mind that nobody else knows about (say 3567), you can add the random number to your PIN code, and communicate the number 5927. The receiving party then simply subtracts 3567 for getting back the PIN code. Information theorists can prove that if this number is truly random, and if you use it only once, that it is impossible to eavesdrop on this communication. The random number is in this case called the cryptography key, and all secure commutation protocols boil down to setting up a situation where the sender and receiver have a suitable key. It is good to remember this for later on when we discuss the quantum version of encryption: All the sender and receiver need to do is to generate a large random number that they both know, while nobody else knows it.

Nowadays on the internet, most encryption is based on the RSA algorithm for public-key cryptography. The key is generated by exchanging a few numbers in a smart order [1]. These are special numbers, chosen in relation to the mathematics of factorizing a number into its prime factors. The security of the algorithm is based on the fact that 9749 x 7753 (multiplication of two prime numbers) is an easy mathematical problem, while it is much more difficult to find these two prime numbers if you are only given the product (in this case 75583997, go ahead and try it). In practice they use much larger prime numbers. However, there is no mathematical proof that finding the two prime factors of 75583997 is much harder than doing the multiplication 9749 x 7753. So, there is no mathematical evidence that the current encryption system for the internet is secure. And there is even some slow but steady and worrisome progress under mathematicians that aim to understand how one can efficiently factorize a big number in its prime factors. For example, the science pages of NRC Handelsblad of 11 & 12 Feb. 2006 report about a brilliant mathematician from China. She found a way to crack the codes that were then used on the internet in $2^{39}$ computational steps (one day of work on your laptop) instead of the $2^{64}$ steps of the fastest protocol till that discovery (about $2^{25}$ days of waiting time if you only have one laptop). For the time being this is simply solved by using larger prime numbers, but there is clearly a need for a protocol that is more fundamentally secure.



## Quantum cryptography

Here quantum mechanics can help. And while many ideas in quantum information science did not yet leave the laboratory (with experimentalists that are on track to *maybe* get a breakthrough some ten years from now), quantum cryptography over distances up to about 100 km really works. There are a few small companies that sell the instruments for it, and it is applied at a few places for communication between banks in financial districts. One of the most famous companies in the field is ID Quantique in Geneva, Switzerland, they have an interesting website on their products and the physics behind it [2,3].

Quantum cryptography uses several of the most fundamental aspects of quantum physics. For example, the fact that it is impossible to measure an unknown quantum state without disturbing it. Or that we can only predict the probabilities of measurement outcomes, while it is impossible to predict one particular measurement outcome. And this latter aspect can only be applied if we already have a lot of information about the quantum state, which an eavesdropper typically does not have. Derived from this, it can be shown that it is impossible to make a copy of an unknown quantum state (no-cloning theorem). In addition to this, some proposed protocols use quantum entanglement (the aspect quantum physics that became famous through the Einstein-Podolsky-Rosen paradox).

Let's illustrate this with a simple physical system in mind. Let's communicate through an optical fiber. We will send individual photons, one at the time. We will only use photons with linear polarization, but that still leaves a lot of playground for interesting quantum physics. The quantum state that describes the polarization is now always in the form $|\Psi\rangle = \alpha|H\rangle + \beta|V\rangle$. The probability amplitudes $\alpha$ and $\beta$ are in this case real and obey $|\alpha| \leq 1,\ |\beta| \leq 1$ and $\alpha^2 + \beta^2 = 1$. The states $|H\rangle$ and $|V\rangle$ are two basis states (and a complete set), which represent states with linear polarization along the horizontal and vertical axis in the labs of the sender and the receiver. They can for example agree that $|H\rangle$ represents a 1 in digital information, and that $|V\rangle$ represents a 0. However, they can also switch to using two other orthogonal states: for 1 the state $|\Psi_{1-45}\rangle = (|H\rangle + |V\rangle)/\sqrt{2}$, and for 0 the state $|\Psi_{0-45}\rangle = (|H\rangle - |V\rangle)/\sqrt{2}$ (in the lab this means they simply need to rotate all the polarization optics for the sending station and detection station by 45 degrees). This simple physical system underlies the so-called BB84 protocol (proposed by Charles Bennett and Gilles Brassard in 1984), and also lies at the heart of the quantum cryptography systems that you can now buy commercially.

Let's shortly discuss the main aspects of the BB84 protocol for illustrating the fact that quantum physics can make communication fundamentally secure. How does it work? The sender and receiver (from now on named Alice and Bob, respectively, according to a widely accepted convention in quantum information science) do the following. Alice just starts sending out a random string of 1's and 0's, while also randomly rotating her polarization optics back and forth all the time over 45 degrees. She writes up what she sent out (1 or 0) for each photon. Bob is detecting all the incoming photons, and tries to measure whether it is a 1 or a 0. He also randomly rotates his polarization optics back and forth all the time. They exchange in this manner a very large set of photons, but that can happen in a few seconds in practice. In this series, it's only half the time that Alice and Bob are sending and detecting 1's and 0's in the same basis (indeed, just by accident). For the other half of the events they were not working in the same basis (one had the basis rotated over 45 degrees with respect to the other). They keep track of their polarization settings as a function of time, and after sending all the photons, they make a phone call and discuss what basis they had in use for each photon (or they use computers to do this automated). They do so *without mentioning the associated value 0 or 1*, so it is no problem if an eavesdropper listens in on this phone call. Then, they just throw away all events for which they were not working in the same basis. What they are left with is an identical string of 1's and 0's at each location that is also a long random number. From this string, they will only use half of the 1's and 0's for the cryptography key. But before doing so, they first use the other half of the bits for a security check. For this check, Alice picks half the bits from the string. She does this at random locations in the string, and tells Bob both the location and bit value for each case. Bob compares this to his string. If all results are identical, they can trust the key with very high probability. If there are differences, they know that something went wrong, and it could mean that an eavesdropper has been trying to listen in (while the eavesdropper made sure that Bob still got the right amount of photons at the right times, but he cannot always give the photons the right polarization).

OH ALICE... YOU'RE THE ONE FOR ME
BUT BOB... IN A QUANTUM WORLD HOW CAN WE BE SURE
ψ+ or ψ- ?

Why is it impossible to eavesdrop on this communication? The eavesdropper cannot for all pulses measure the polarization state of a single photon without disturbing it, or in a way that he gets the right answer (1 or 0) with certainty. The reason is that he does not know in what basis he should measure (normal, or 45 degrees rotated). Say Alice sends a 1 in the rotated basis (she sends the state $|\Psi_{1-45}\rangle = (|H\rangle + |V\rangle)/\sqrt{2}$), and the eavesdropper happens to measure in the non-rotated basis. The laws of quantum mechanics then say that he can then get the answer H with 50% probability, or V with 50% probability. He can only get these distinct answers, and he can never get certainty what the polarization state was before his measurement. Let's assume he measured V. The best he then can do to hide his actions is to still send a photon to Bob very rapidly with polarization state $|V\rangle$. However, Bob (if he happens to measure in the same basis as Alice) will then detect a 0 instead of a 1 with 50% probability. So, when this is applied to a long string of bits, Alice and Bob will later find out that they have different bit values for many bits, even when they measured in the same basis.

## Current research in the Quantum Devices Team and elsewhere

So, BB84 works in practice. Does this mean that research into quantum communication is finished? No, it is rather the opposite. One problem, for example, is that there are no cheap, stable and tunable optical emitters that can deliver a single photon on demand. In practice, one now works with very weak laser pulses. But these then often contain (as it turns out after measurement) zero photons. And, a small fraction of the pulses then has two photons, or even three. This makes the implemented BB84 protocol less secure than the ideal one.

Another problem is that one cannot amplify the optical signals on the way without disturbing the quantum state. In practice, this means that BB84 cannot be applied for distances over 100 km (both for optical fibers and propagation through air), simply because the probability that a photon gets lost on the way gets very high after 100 km. The research in my group carries out experiments that aim to tackle this problem by trying to build a so-called quantum repeater with electron spins in semiconductors.

The quantum repeater helps to realize quantum communication over distances larger than 100 km in an efficient way [4,5], efficient means that the required resources and time do not grow exponentially with distance). The communication channel is now divided in segments of 100 km, and at each node there is a quantum memory element for photons. We try to implement this with tiny semiconductor devices. The idea is that the spin of an electron can be in a quantum superposition of spin-up and spin-down. We try to implement that during the absorption of one photon by a semiconductor device, the photonic quantum state is transferred to the quantum state of the electron spin. This does not violate the no-cloning theorem, since the optical pulse is gone after the absorption process. Also note that the electron spin can now carry the quantum state, while operating this process does not reveal the quantum state (that is, it is not a measurement process). In a second step, we aim to operate the inverse process: operate the semiconductor as a light emitter, where the quantum state of the spin is transferred back to the quantum state of an optical pulse. These are exciting experiments, and you are welcome to drop by our labs for further questions, an update, and a cup of coffee. •

Caspar van der Wal (Netherlands, 1971) obtained his PhD degree in 2001, in the group of Prof. Hans Mooij at Delft University of Technology for research on quantum coherent dynamics of superconducting circuits. This was followed by a postdoc position of two years in the labs of Prof. Misha Lukin and Dr. Ron Walsworth at Harvard University (USA), where he did research on quantum optics with atomic vapors. At the end of 2003, he started working as an assistant professor at the University of Groningen in the Physics of Nanodevices Group. In 2009, he obtained here a permanent position as associate professor in 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. For his current research he obtained the NWO-Vidi Grant (2005) and the ERC Starting Grant (2011).

## Referenties

[1] http://en.wikipedia.org/wiki/RSA_(algorithm)
[2] http://www.idquantique.com/
[3] http://swissquantum.idquantique.com/?Key-Sifting
[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] Towards quantum optics and entanglement with electron spin ensembles in semiconductors, Caspar H. van der Wal, Maksym Sladkov, Solid State Sciences 11, 935 (2009).