Quantum technology in critical infrastructure protection

M. Karol & M. Życzkowski
Institute of Optoelectronics, Military University of Technology, Poland

Abstract

Finding effective ways of critical infrastructure object protection requires more recent and more sophisticated security systems. Particularly important security aspects are information protection and perimeter security. Development of a new quantum technology, both in quantum computing and quantum cryptography, gives the necessary technology needed to build single photon optic fiber systems. The authors would like to present concepts of using single photon interferometers to protect infrastructure facilities which, in particular, take into account optical fiber transmission lines. The conducted analysis of what is available on market systems and the expected single photon sensor's properties in terms of security and information show a drop in detection. We also compared the degree of systems' complexities in terms of system security and difficulties associated with devices' construction and installation in transmission lines.

The paper presents the main principles of single-photon interference, the operation and construction of single photon systems in the detection and generation of single photons for the purpose of commercial systems. The concept will be described as perimeter protection and the protection of a transmission line by a single photon sensor. The authors discuss the proposed construction and operation of the proposed fiber optic single photon interferometer as a protection sensor. They also try to bring the possibility of using the sensor in areas other than the protection of transmission lines and compare the predicted properties of single photon sensor currently implemented solutions in the field of fiber optic sensors for perimeter protection.
Keywords: single photon, QKD, security, critical infrastructure.

WIT Transactions on The Built Environment, Vol 151, © 2015 WIT Press
www.witpress.com, ISSN 1743-3509 (on-line)
doi:10.2495/SAFE150101

1 Introduction

As a critical infrastructure we must consider systems and their constituent functionally interconnected objects, including building structures, equipment, installations, services essential to safety of the state and its citizens in order to ensure the smooth functioning of public administration, as well as institutions and entrepreneurs. With a view to crisis management law, data transmission infrastructure between government departments can be assigned as a critical infrastructure requiring special protection.

Rapid development of computing power makes it difficult to generate safe encryption key and efficient encryption algorithms to protect classified information. The constant increase of the transmitted data rate increases difficulties with ensuring data safety in growing data volume transmission. In addition, technology development of quantum computers' construction creates a security risk for almost every existing encryption algorithm.

Therefore, in order to ensure classified information transmission safety it is necessary to apply "one time pad" algorithms which use an encryption key only once, and the key is of the same length as the transmitted massage. This algorithm is proved to be unconditionally safe, but its use is limited due to a required length of encryption key. Since the encryption key must be of the same length as the transmitted message, and current generation methods do not provide sufficient length of the generated key, it causes serious problems with the use of "one time pad" during broadband communications. A solution to this problem may be quantum key distribution (QKD) systems. Further development of this technology could make it possible to apply the encryption algorithm with a one-time used key. At present, the key generation rate by QKD systems goes to hundreds of Kbps. In such a case, although a bandwidth is important, the strength of a generated key is however crucial to full message safety and makes the decryption of a massage received without complete knowledge of the encryption key impossible.

Security of QKD systems is based on a quantum mechanics' basis which, according to current knowledge and theoretical assumptions, cannot be broken. Moreover, the key distribution protocol called BB84 [1] has been mathematically proven to be absolutely safe [2, 3]. It can be concluded that a combination of unconditionally secure encryption algorithms with the key generation will allow us to get a fully secure message encryption.

Unfortunately, a real implementation of this method has many limitations on side of quantum key generation methodology. A team of authors conducted a series of tests and analyses revealing opportunities and ways for current systems to protect systems from breaking their safety. Moreover, the possibility of using single photon systems in terms of critical infrastructure security was explored. In that capacity, a concept was developed and preliminary tests were carried out to monitor the state of transmission lines using a single photon interferometer. The assumption of the use of quantum mechanics' principles guarantees a possibility of external disturbances' detection in transmission lines with an accuracy exceeding currently used systems.

2 Specific properties of single-photon technology

In quantum mechanics we talk about possible states rather than exact values. In a simpler way we can say that we want to find a place where there is a particle which we are particularly interested in. But it is impossible to find the exact particle position; only the place where it can most likely to be found, but not necessarily a place where the particle is in reality. This is a consequence of the inability to make accurate measurements in accordance with Heisenberg's uncertainty principle.

Thanks to the properties of quantum mechanics, among others, it is possible in practice to use a single photon as a completely safe data carrier. Because, in accordance with Heisenberg's uncertainty principle and Bell's theorem, it can be determined whether quantum information has been eavesdropped. This is possible by coding information in a photon with the use of one of two features. Unfortunately, information coded in a single photon can be read out, but reading it gives information about eavesdropping.

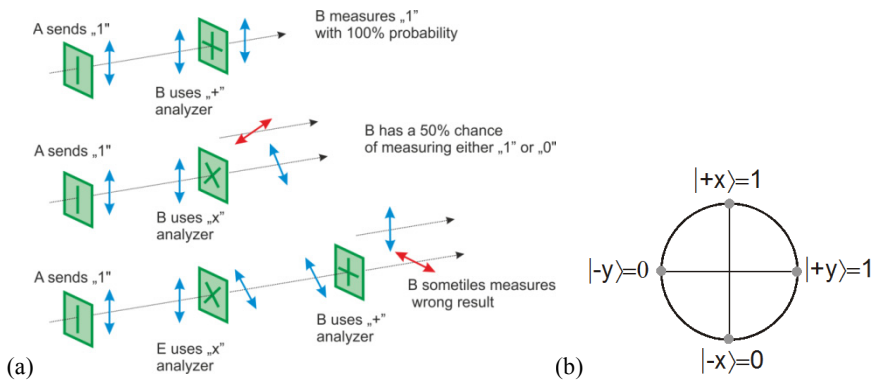

Figure 1: (a) Measurements of polarization states; (b) bit values of polarization states.

The first feature allowing the use of a single photon as a data carrier is the polarization state. Use of orthogonal polarization states for coding values "0" and "1" allows for distinguishing between these states by simple passage of a photon through a polarization beam splitter. Such approach is schematically presented in fig. 1(a). It is possible to generate such polarization state that, after passing through the same polarization beam splitter, it will pass a photon on one of two outputs with equal probability. Furthermore, coding with the use of two bases rotated relatively to each other by 45 degrees allows us to diversify a single-bit coding method by using two distinguishable states of polarization (fig. 1(b)). Using an incorrect polarization analyser will cause the appearance of transmission errors. Eavesdropping and wiretapping is revealed by an increase of quantum bit error rate measured at the receiver's signal.

Such an approach of using polarization encoding is in accordance with original assumptions of BB84 protocol. In this approach, photon bits are encoded by using linear polarization states (fig. 1(a)) and measured by using two analysers (fig. 1(b)). Since it is not possible to measure four polarization states at the same time, and the measurement with a wrong base changes the photon state with a 50% probability, the measured values may be different from the transmitted ones.

Similarly, it is possible to encode information in a photon phase by using single-photon interference. According to the principle of single-photon interference (1)(2) based on a phase difference between signals in individual interferometer arms, the probability of photon detection at different outputs changes.

$$-r^2 e^{i\Theta}|\Psi> + t^2 e^{i\varphi}|\Psi> = t^2 - r^2(e^{i\varphi} + e^{i\Theta})|\Psi> \quad (1)$$

$$irte^{i\varphi}|\Psi> + irte^{i\Theta}|\Psi> = irt(e^{i\varphi} + e^{i\Theta})|\Psi> \quad (2)$$

$$\Theta = \varphi: \begin{cases} 0 \\ |2irte^{i\varphi}|^2 = 4r^2t^2 \end{cases} \qquad \Theta - \varphi = \pi: \begin{cases} 2(t^2 - r^2)e^{i\varphi} \\ 0 \end{cases} \quad (3)$$

where $t|\Psi\rangle$ and $r|\Psi\rangle$ are states of photon in interferometer arms; φ and Θ are phases of radiation in interferometer arms.

In the single photon interferometer system shown in Fig. 2 for the phase difference of 0 and π, there is a certainty of photon detection on one detector (3). So the signal phase shift of π between branches is used to code bit states of "0" and "1" which correspond with orthogonal polarization states.

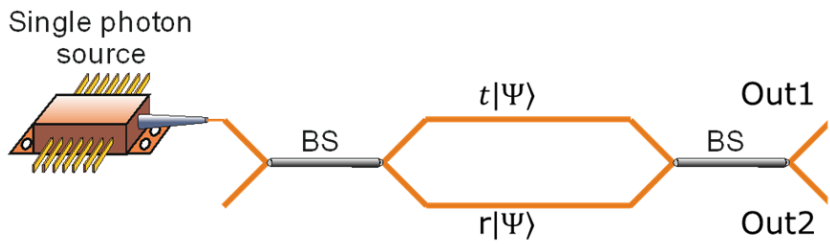

Figure 2: Single photon interferometer scheme.

A polarization coding system based on quantum mechanics is regarded as a foundation of quantum information transmission, while, at the same time, describing the technique in the most intuitive way. However, difficulties of sending a polarization state by an optical fiber transmission medium make commercial use of polarization coding a very complicated issue. Phase coding is also based on principles of quantum mechanics and single-photon interference,

but systemic implementation allows to use this encoding in real commercial systems.

Information transmitted through a classic telecommunications' channel can be amplified or copied by using commercially available equipment. Quantum states of photons transmitted through a transmission medium in accordance with no cloning theorem cannot be copied without measuring the photon state, because each measurement can distort the transmitted photon state what may be giving an incorrect measurement result in the receiver. This ensures inability to eavesdrop the transmitted massage by a third party while ideal optoelectronic components are used in the transmitting and receiving devices.

Both polarization or phase changes made to a transmission medium are easy to observe. The most common effect observed in the case of a disturbed transmission line is the appearance of detection at wrong detectors. This allows for an accurate detection of disturbances in an optical fiber which transmits a photon by using a relatively simple method of signal processing and generating an alarm signal that causes repeated generation of the encryption key. This solution is currently used in available commercial devices.

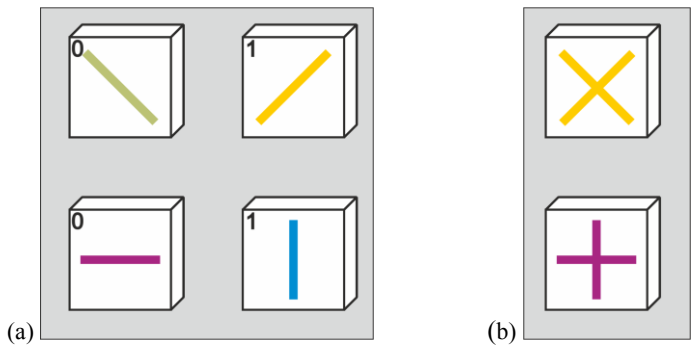

Figure 3: (a) Polarization states; (b) BB84 analysers.

In order to improve the properties of quantum systems, it was necessary to eliminate some of the problems associated with transmission of radiation through an optical fiber. The biggest problem in transmission is a random change occurring in transmitted light polarization. Thus, it was necessary to develop a system compensating for environmental impact to changes introduced to polarization in a transmission line. Construction of an auto-compensating phase device is shown in fig. 4. This system is composed of two devices called the transmitter (Alice) and receiver (Bob). The transmitter is built with a Faraday rotator mirror, phase modulator coupled with a random number generator, variable optical attenuator (VOA) and sync detector. The receiver consists of two single photon detectors, a sub-nanosecond laser, a phase modulator coupled to two random number generators, an unbalanced Mach-Zehnder interferometer and control system.

Although the radiation source is located in the same system as single-photon detectors, it is not a transmitting device. A transmitting arrangement is

considered a device in which attenuation of a strong laser pulse to a single-photon level is carried out and one of four states is encoded by a phase modulator. The receiver's and transmitter's fiber optic elements are made of polarization maintaining components which enable an interferometric system's balance. A sub-nanosecond pulse generated by a pulse laser is initially divided into two beams using a 50/50 beam splitter at unbalanced interferometer input. In the short arm, an optical fiber is spliced with 90° optical axes' rotation ensuring orthogonal polarization states in both arms. Then, the polarizing beam splitter combines radiation from both arms to one transmission fiber. Radiation coming out from the device is in the form of two time-shifted pulses. Pulses propagate through the fiber to the receiver where an asymmetric beam splitter decouples light to a synchronizing detector. The rest of the radiation passes through a variable attenuator, an inactive phase modulator and, at the end of the fiber, is reflected from a Faraday rotator mirror. After reflection, radiation makes another pass by the phase modulator which, this time, introduces change (compatible with values generated in RNG) to the second pulse. Then, radiation passes for the second time through the variable attenuator which makes attenuation set at half value required to obtain a single photon in pulse. FRM at the system's end ensures rotating polarization causing that radiation from a shorter arm will be propagating in a longer arm and vice versa. As a result, automatic compensation of environmental influence on the optical fiber is obtained. In the interferometer's shorter arm there is a phase modulator which introduces changes to a returning pulse. Depending on phase changes, a signal is obtained at one of single photon detectors according to the single photon interference rule.

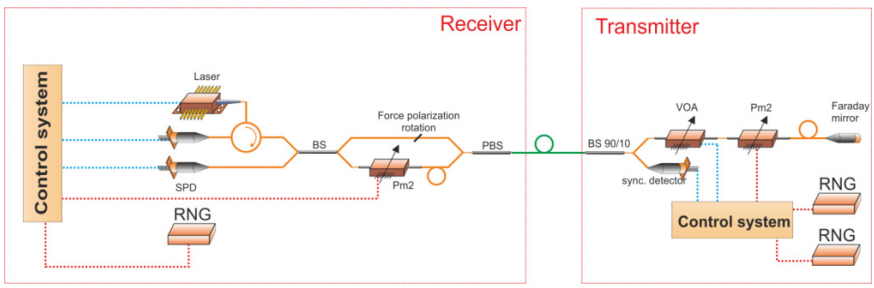

Figure 4: Auto-compensating phase system scheme.

These systems for both phase and polarization configurations have drawbacks and limitations which, for polarization configuration, are the following:

- Fiber optics change polarization stochastically;
- Reduction of speed and accuracy by polarization controllers;
- Requires the use of up to four single photon detectors;

while in systems based on phase we can distinguish the following disadvantages:

- Light polarization affects output result;
- Balanced interferometers are required;
- Backscattering (in some configurations);
- Speed of phase modulators.

3 Quantum detection limitations

When using single-photons in an optical path there are many problems associated with detection and generation systems. This is due to many factors, both technological and physical properties. The research and analysis conducted by the authors show that components used in quantum key distribution systems have a number of imperfections. Those imperfections have a significant impact on key security and generation rate.

Detectors are one of the most important components in quantum systems. At present, detectors are used in various types which achieve the best efficiency reaching up to 95% [4]. Unfortunately, they work at temperatures close to absolute zero. Therefore, InGaAs avalanche photodiodes are the most commonly used detectors which allow us to work at room temperatures using a thermoelectric cooler. Many factors have an influence on detectors' performance, starting with construction of a detecting element, detector operation temperature and control voltages. Changes in individual parameters allow us to get different photon detection efficiency with a different noise level. Currently, detection efficiency of APD diodes reaches up to 25%, but these values are still too small for telecommunication application. In addition, more "false counts" appear at higher efficiencies because of an increase in the threshold voltage, so there is no gain in usable pulse detections. An important aspect of single-photon detection is not only to obtain the highest efficiency, but also to minimize false detections. Therefore, while using detectors in systems a constructor should seek to obtain the optimal value of detection probability and detector's noise.

As mentioned before, physics' operation of detectors has an effect on single-photon detection. The most effective method to counteract these effects is the selection of control parameters of the detector. This concerns:

- the detectors' own noise;
- false counts;
- a strong possibility of blinding detector by strong laser radiation [5];
- the possibility of counting by the detector photons from the optical path not related to the transmission channel.

4 Single photon generation

A single photon source in telecommunication applications should be characterized by the following parameters:

- Emits only one photon – high p(1) emission probability, low p(2) and p(0) probability;
- Narrow spectral width – small $\Delta\lambda$;
- On demand – triggered;
- Room temperature operation;
- Low cost.

At the moment, there is no single-photon source to meet all of these conditions. Very good methods are the following: "Heralded single photon source (down-conversion) [6]", "Emission from Nitrogen Vacancy Center in Diamond [7]" and "Quantum Dot in Micropost Microcavity [8]". The single-photon source with good generation performance requires very low operating temperatures and high costs. There are no radiation sources allowing efficient single-photon generation at room temperature. Since commercial sources are used in the operating room conditions of low cost construction, the attenuated laser pulses' method is used in available devices.

In order to obtain a single photon from a laser pulse it has to be attenuated, but the attenuation level is dependent on laser power and the expected number of photons in a pulse. According to Poisson distribution, attenuated pulse photons are generated with a certain probability depending on the expected number of pulses. To avoid the occurrence of more than one photon, it is necessary to set the attenuation system to an expected value of 0.1 photon per pulse which means that probability of an emitting photon in a pulse is approximately 9.5%. To determine the required attenuation level to reach a desired value, continuous measurements of source generated radiation are required. These measurements are shown in fig. 5. The mean value of radiation source power allows for the estimation of required attenuation level allowing us to obtain single photons with a very low probability of occurrence of pulses consisting of more than one photon.

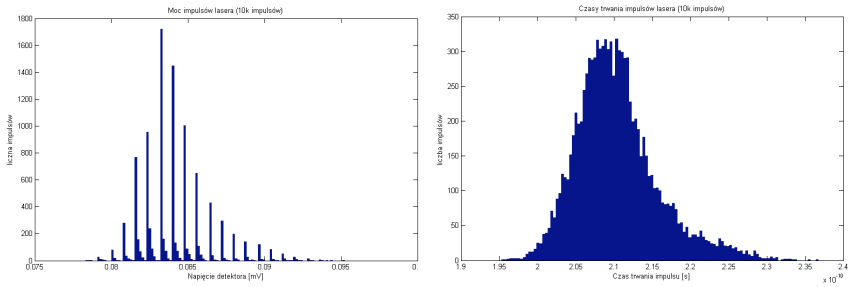

Figure 5: Pulse time and power distribution of laser pulses.

Due to the stochastics of single photon measurements' processes correct result interpretation requires a proper attitude. With a generation of laser pulses at a frequency of 100 kHz, in fact, after attenuation, only 9.5k single photon pulses per second can be used for encoding information. Further, after detection with efficiency about 20% and 1μs detector dead time, the amount of single photon pulses is reduced practically up to 900 pulses per second.

Elements responsible for encoding information are a very important component in quantum key transmission. These elements limit key exchange systems' speed by the time needed to switch between different coding states. It is also extremely important to obtain repeatable modulators' settings in order to avoid errors of incorrect coding or reading transmitted photons.

While using an optical fiber as a transmission medium a significant reduction of systems' throughput occurs caused by fiber optic attenuation. For example, the probability of a single-photon transmission at a distance of 1 km is about 63%, and the maximum theoretical range is up to 400km [5]. Moreover, when auto-compensating systems are used, there is a risk of single photons generated by partial reflection and backscatter from fiber connectors or imperfections. Elimination of this phenomenon is realized by the addition of storage fiber on the transmitting device. Also key information packets are transferred to detect reflected pulses when there is no right for photons reflected from the fiber imperfections to appear.

The impact of all components and processes for key generation efficiency significantly reduces encryption performance of quantum key exchange systems.

5 Vulnerability of QKD systems

The most spectacular attack on quantum key exchange systems was the attack [9] performed on an operating polarization system at the University of Singapore. During that attack, a method of blinding and controlling single photon detectors [10] with suitable powers' radiation was used. The attack was carried out on the basis of photons received by a duplicate of the receiving apparatus from the trusted side. The eavesdropper device using circularly polarized radiation blinds the receiver enforcing linear work of single photon detectors. Then, by using a strong pulse, the eavesdropper measurement result is forced on the receiver at the trusted side. This pulse in each case ensures detection on the appropriate detector. The attack remains undetected by regular techniques due to the use of a real receiving system as part of an eavesdropper device which allows for achieving the effect of a complete link of the quantum key distribution. The scheme of the system used to conduct this attack is shown in fig. 6.

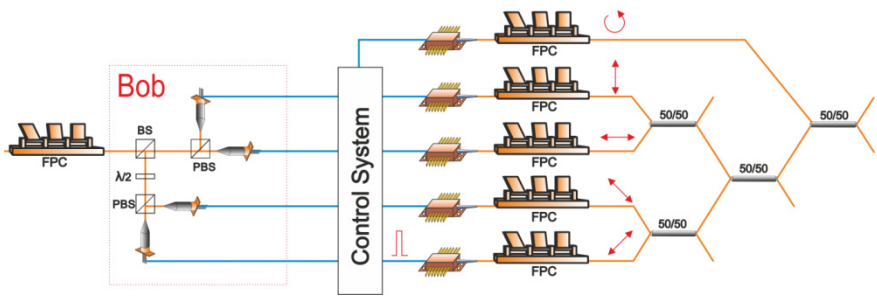

Figure 6: Scheme of QKD eavesdropping device.

Other well-described attacks are Trojan-horse attacks [11, 12]. They are carried out on the basis of sensing the phase modulator state using reflected signals within a transmitting system using the OTDR technique. In this attack the aim of the eavesdropper is not to measure a single photon state, but to get a

strong light pulse identical state as the coded photon. For this purpose, the eavesdropper is plugged into a transmission line and a strong radiation impulse is sent to the transmitter. Reflection from transmitting system components passes through a phase modulator at the same time as a single photon. Consequently, the eavesdropper obtains full information about the coded signal with no need to decode the disturbance of the single photons' state.

In addition to defined and tested attacks, there are many presented theoretical methods of attacks on quantum systems. In this group, there are risks related with prepared assumptions of technologies' development, such as:

- Photon Number Split attacks which assume the use of quantum memory for storing pulses of photons with a population greater than one [13].
- the possibility to make non-destructive measurement of the transmitted photon state [14].

As shown, despite theoretical evidence of security, implementation of components in a real system remains a problem. Current implementations have limitations and weaknesses which are still detected and corrected. Patches introduced by manufacturers against individual attacks seem to be an effective solution, but they are not included in system security models. Therefore, the question is whether these systems are safe enough?

6 Conclusions

At the present moment, quantum cryptography systems can increase security of transmitted data with keeping adequate precautions. However, due to the lack of security evidence for such transmission, systems' application to classified information protection is currently impossible. Moreover, a crucial value in telecommunications is the amount of transmitted data. Current solutions significantly reduce the capacity of quantum key exchange systems. Further development of technology may improve transmission rate and its security allowing us to use security applications at a government level. Research on quantum computers can make most classical encryption systems unsafe and, thus, it can force a development of more advanced coding techniques than those used so far. Therefore, it will be necessary to develop technologies which will ensure the safety of key exchange and data encryption. This task can be performed by the technology of quantum key exchange, if the major problems of detectors and other components are solved.

Acknowledgements

The project is co-financed by the National Centre for Research and Development within the project realized for national security and defence "Fiber-optic link integrity monitoring system for protection against unauthorised access to classified information" (System monitorowania integralności łącza światłowodowego w celu ochrony przed nieautoryzowanym dostępem do informacji niejawnych), Contract no. DOBR/0070/R/ID1/202/03.

References

[1] C. H. Bennett and G. Brassard, Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, 175–179 (1984)
[2] P. Shor, J. Preskill, Phys. Rev. Lett. 85, 441−444 (2000)
[3] H. K. Lo, H. F. Chau, Science 283, 2050–2056 (1999)
[4] A. E. Lita, A. J. Miller, and S. W. Nam, Opt. Express 16, 3032 (2008)
[5] Quantum communication technology N. Gisin and R. T. Thew Electronics Letters, 46, 965 (2010)
[6] S. Fasel, O. Alibart, S. Tanzilli, P. Baldi, A. Beveratos, N. Gisin and H. Zbinden, New Journal of Physics 6, 163 (2004)
[7] C. Kurtsiefer, S. Mayer, P. Zarda, and H. Weinfurter, Phys. Rev. Lett. 85, 290 (2000)
[8] M. Pelton, C. Santori, J. Vučković, B. Zhang, G. S. Solomon, J. Plant, and Y. Yamamoto, Phys. Rev. Lett. 89, 233602 (2002)
[9] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Nat. Photonics 4, 686–689 (2010)
[10] V. Makarov, N. J. Phys. 11, 065003 (2009)
[11] A. Vakhitov, V. Makarov, and D. R. Hjelme, J. Mod. Opt. 48, 2023–2038 (2001)
[12] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy,Phys. Rev. A 73, 022320 (2006)
[13] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders. Physical Review Letters, 85(6):1330+ (2000)
[14] A. Reiserer, S. Ritter, G. Rempe, Science 342, 1349 (2013)