High-speed free-space quantum key distribution system for urban daylight applications

M. J. García-Martínez,1,* N. Denisenko,1 D. Soto,1 D. Arroyo,2 A. B. Orue,1 and V. Fernandez1

1Information Security Institute, Spanish National Research Council (CSIC), Serrano 144, Madrid 28006, Spain
2Grupo de Neurocomputación Biológica, Dpto. de Ingeniería Informática, Escuela Politécnica Superior, Universidad Autónoma de Madrid, Madrid 28049, Spain
*Corresponding author: mariajose.garcia@iec.csic.es

Received 19 February 2013; revised 11 April 2013; accepted 16 April 2013; posted 17 April 2013 (Doc. ID 185412); published 7 May 2013

We report a free-space quantum key distribution system designed for high-speed key transmission in urban areas. Clocking the system at gigahertz frequencies and efficiently filtering background enables higher secure key rates than those previously achieved by similar systems. The transmitter and receiver are located in two separate buildings 300 m apart in downtown Madrid and they exchange secure keys at rates up to 1 Mbps. The system operates in full bright daylight conditions with an average secure key rate of 0.5 Mbps and 24 h stability without human intervention. © 2013 Optical Society of America

OCIS codes: (270.5568) Quantum cryptography; (060.2605) Free-space optical communication.

http://dx.doi.org/10.1364/AO.52.003311

1. Introduction

Quantum key distribution (QKD) [1] uses physical properties of single photons, such as polarization or phase, to securely distribute cryptographic keys between two parties. It emerged as an attempt to solve the problem of key distribution by uniquely detecting the presence of an eavesdropper in the communication channel via the Heisenberg uncertainty principle.

QKD has greatly evolved since the first experimental demonstration in 1992 [2] and distances up to 144 km in free space [3] and 250 km in optical fiber [4] have successfully been achieved. Free-space quantum communications for long-haul applications will play an important role in securing earth-to-satellite links [5]. For shorter-distance applications located in urban scenarios, free-space QKD could be an interesting alternative for commercial, government, and financial institutions that wish to be securely connected to the backbone of metropolitan networks without the licensees required in fiber optics solutions and with higher portability and flexibility in terms of installation.

One critical issue when using the atmosphere as the transmission channel is that extraneous background light can couple into the receiver leading to an increased error rate. Some free-space QKD systems that implement efficient methods to reduce background radiation, enabling the operation in daylight conditions, have been demonstrated in [6–10].

Another aspect of free-space QKD implementations that needs special attention is turbulence in the atmosphere, which can lead to beam spreading, beam wander, and scintillation at the receiver. The effect of such link fluctuations on free-space decoy-state QKD has been recently studied in [11].

In [12] a thorough review of latest most representative free-space QKD experiments is performed. It shows that, though great advances have been reported [13], the transmission bit rates of present experimental realizations of free-space QKD are still low, limiting their implementation for real-world applications.
Two low-absorption atmospheric spectral windows in the near-infrared regions of $\lambda \sim 850$ nm and $\lambda \sim 1550$ nm are usually considered for free-space optical communications. Although the latter wavelength has an associated higher transmission and it is slightly less affected by turbulence effects and backscattering, detection technology must also be considered. Indeed, while InGaAs single-photon detectors have greatly improved their performance in terms of the maximum repetition rate they can operate at (from megahertz to gigahertz) [14], they are still outperformed by commercially available Si single-photon detectors (Si-SPADs) in critical parameters, such as dark-count rate, detection efficiency, and afterpulse probability. Likewise, superconducting single-photon detectors, although exhibiting low timing jitters and dark-count rates at $\lambda \sim 850$ nm [15], still exhibit lower detection efficiencies than Si-SPADs, and must be cooled down to temperatures as low as 3 K. Therefore, a source wavelength of $\lambda \sim 850$ nm in conjunction with Si-SPADs as the single-photon detectors was chosen as the most efficient and practical solution to achieve gigahertz clock rates [16].

In this paper, we present a free-space QKD system that implements the B92 protocol [17] at gigahertz clock frequencies over a distance of 300 m in Madrid. Several experiments have been performed to determine the system’s optimum clock frequency, the influence of solar radiation, and the system’s stability and robustness to misalignment. The QKD system and its characterization will be described in detail in the next two sections.

2. Experimental Setup
The emitter setup of the proposed free-space QKD system is shown in Fig. 1. The purpose of the emitter module is to send out single photons carrying information codified in their polarization state. In order to emit individual photons the sender heavily attenuates a laser source, thus emitting the so-called weak coherent pulses that follow a Poisson distribution. To achieve high transmission rates Alice uses a fast gigahertz pulse pattern generator in conjunction with vertical-cavity surface emitting lasers (VCSELs) controlled by high-speed drivers, which can operate at several gigabits per second. Both VCSELs emit at a central wavelength of 848 nm, with an FWHM spectral bandwidth of 45 pm. The driver of each VCSEL contains an automatic power control circuitry, which maintains an average optical power output and ensures a stable wavelength emission over changes in temperature and laser properties.

Each laser output is coupled into a single-mode optical fiber at $\lambda \sim 850$ nm, which spatially filters the beam ensuring that only one spatial mode is propagated. Each fiber output is then connected to a fiber-coupled attenuator to reduce the average number of photons per pulse to $\mu \sim 0.1$, which guarantees that only 0.5% of the emitted pulses contain more than one photon per pulse. Higher values of $\mu$ can be used if a decoy-state protocol is implemented, as reported in [18]. The output of each attenuator is collimated and launched into two high extinction-ratio polarizers to produce the polarization states required by the B92 protocol. These states are combined by a nonpolarizing beam splitter cube. Timing synchronization between emitter and receiver is carried out by another laser beam emitting at $\lambda \sim 1550$ nm, which conveys Alice’s internal clock signal to Bob. The use of a classical channel operating at a different wavelength in parallel with the quantum channel has already been implemented in [9,19]. If done with sufficient timing precision, this technique does not decrease the speed of the system, since no further software compensation is needed due to emitter and receiver having exactly the same
clock. The synchronization signal is then combined with the two $\lambda \sim 850$ nm beams by a broadband pellicle beam splitter. Both $\lambda \sim 850$ nm beams are then collimated and expanded to a diameter of $\sim 40$ mm by using a set of two achromatic lenses. The transmitter is mounted on a high-precision gimbal system, which facilitates the alignment and pointing with the receiver.

The receiver is located at approximately 300 m from the transmitter. This unit consists of a telescope, the receiver’s optics, two silicon single-photon detectors, an InGaAs photodetector and a timestamp card. A photograph and a diagram of Bob’s module are shown in Fig. 2.

The beam coming from Alice is focused by a Schmidt–Cassegrain telescope with an aperture diameter of 25.4 cm. The receiver’s optics have been designed to be directly coupled to the output of the telescope. A half-wave plate at the input of the receiver’s optics is used to align the incident electric field of the two nonorthogonal states with the transmission axis of Bob’s dichroic mirror to minimize degradation of the polarization states. The beam at $\lambda \sim 850$ nm and the “synchronization beam” at $\lambda \sim 1550$ nm are then spectrally discriminated by a dichroic mirror. The solar background radiation is filtered by using a narrow bandpass spectral filter centered at $\lambda \sim 850$ nm.

The discrimination of the two nonorthogonal states encrypting the binary states “1” and “0” is achieved by using two high-extinction (>10000:1) polarizers. The procedure is as follows: Bob performs measurements on the photons with either of the two polarizers (see Fig. 2), which sometimes fail to detect a “click” (the polarizer is oriented to block the photons of the unwanted polarization state), but when a measurement succeeds it always provides the bit correctly—note that under these measurement schemes if Alice transmits a “0” there is no possibility (except for errors due to noise and device imperfections) that Bob measures a “1”, i.e., that he gets a “click” in channel 1, and vice versa. That is, if Bob chooses the wrong polarizer to measure a photon, he will not measure anything, and therefore no errors will be introduced in his bit sequence. Hence, there is no need for reconciliation of basis sets between Alice and Bob to discriminate ambiguous measurements since the string of bits measured by Bob is directly the sifted key, which simplifies this protocol when compared to the BB84 protocol [1].

After the polarizers, the discriminated signals are coupled into multimode fibers, which spatially filter the background radiation collected by the receiver. The photons are then detected by two PerkinElmer SPCM-AQR-12 actively quenched Si-SPADs with a single-photon detection efficiency of $\eta_{\text{det}} \sim 0.32$, and a dark-count rate of $\sim 200$ Hz. The output of each detector is connected to each data channel of the timestamp card, which is used to record the arrival times of the detected photons. The synchronization signal, which is detected by an InGaAs photodetector and amplified by a fast transimpedance amplifier, is connected to the clock input of the timestamp card. It must also be stressed that the detectors used in this work have been the target of a series of attacks by using bright illumination [20]. No satisfactory solution has yet been devised, which emphasizes that a more general security proof incorporating imperfect detectors is needed [21].

A short “known sequence” is sent by Alice at the beginning of every key. This sequence is used by Bob to identify the beginning of his sifted key. Bob

---

Fig. 2. Picture (a) and diagram (b) of Bob’s module. SPD, single photon detectors and APD, an avalanche photodiode; $L_1$, $L_2$, and $L_3$ are three achromatic doublet lenses used to couple the signal into the optical fibers.
sends Alice the bit positions where he detected a photon, and Alice then generates her sifted key from this information. To test for eavesdropping Alice randomly chooses a fraction of the sifted key as test events. For those test events, Alice publicly broadcasts their positions and binary values. Bob then computes the quantum bit error rate (QBER) of the test events, i.e., the ratio of wrong events (those for which his and Alice’s value disagree) to the total number of detected events. If the computed error rate is above a certain value, which for our system is 8%, no secure key can be extracted from the sifted key after the error correction and privacy amplification processes.

Sender and receiver are isolated from stray background light by being covered in blackout material. This reduces the amount of stray light that is coupled in the receiver by more than 1 order of magnitude.

3. Results and Discussion

Experiments were performed with emitter and receiver situated at a distance of 300 m in the city center of Madrid. The transmitter was located in the sixth floor of the Institute of Agricultural Sciences, and the receiver in the third floor of the Information Security Institute, both belonging to CSIC.

All information shared by Alice and Eve, $I_{AE}$, needs to be subtracted from Alice and Bob’s sifted sequences to generate the final secret key. In our case we have considered the worst case scenario where Eve performs two types of attacks on the channel simultaneously: the unambiguous state discrimination (USD) attack [22] and the photon number splitting (PNS) attack [23-24]. It is known that the B92 protocol is vulnerable to the USD with a lossless channel attack, whereby Eve can gain 100% of the key if the loss of the channel is $\geq71\%$ [25]. If the loss of the transmission channel is lower, Alice and Bob can distill a secret key, albeit at the cost of discarding the information gained by Eve through privacy amplification. In our case, the loss of the link is $13.2\%$ at 300 m, allowing an eavesdropper to intercept and perform a USD attack to $18.7\%$ of the photons sent by Alice without being detected. If Eve attacks a higher percentage than this, she will generate a loss that she will not be able to compensate for. By performing a USD attack to $18.7\%$ of the photons transmitted by Alice, Eve obtains $29.3\%$ of them unambiguously [26], which corresponds to $5.5\%$ of the emitted photons. The remaining attacked photons, $13.2\%$, are detected ambiguously, and thus Eve blocks them not to increase the error rate. She now replaces the channel by a lossless one and sends the photons she detected deterministically. Bob does not notice anything anomalous and Eve remains undetected. In addition, we have considered that Eve also performs the PNS attack to all the multiphoton pulses transmitted by Alice. In our case, the information shared by Alice and Eve is then given by

$$I_{AE\text{total}} = I_{AE\text{USD}} + I_{AE\text{PNS}},$$

where $I_{AE\text{USD}}$ is the information shared by Alice and Eve, assuming Eve performs the above mentioned USD attack, and is given by [26]

$$I_{AE\text{USD}} = 0.187(1 - \cos \theta),$$

(2)

$\theta$ being the relative angle between the polarization quantum states (typically 45°). $I_{AE\text{PNS}}$ is the information shared by Alice and Eve assuming a PNS attack is taking place, and corresponds to the fraction of tagged bits, $\Delta$ [27], or bits received by Bob that may have leaked all of their signal information to an eavesdropper without introducing any error. In that case $\Delta$ is given by

$$I_{AE\text{PNS}} = \Delta = \frac{\mu}{\exp(-\eta\mu)} = \frac{1 - (1 + \mu) \exp(-\mu)}{1 - \exp(-\eta\mu)},$$

(3)

$\mu$ being the probability that a multiphoton pulse is emitted by Alice, $\exp(\eta)$ the probability for a non-empty pulse being detected by Bob, $\mu$ the average photon number per pulse, and $\eta$ the transmittance of the channel and receiver combined. Therefore, the final secure key rate ($R_{sifted}$) per second is given by

$$R_{\text{sifted}} = R_{\text{net}}[1 - I_{AE\text{total}}] - f(e)H_2(e) - (1 - I_{AE\text{total}}) \times H_2\left(\frac{e}{1 - I_{AE\text{total}}}\right).$$

(4)

where $e$ is the QBER, $f(e)$ is the efficiency of the error correction process (which we have assumed to be 1.2), and $H_2$ is the binary entropy function. Therefore, to guarantee security, the sifted key rate ($R_{sifted}$) is reduced by $f(e)H_2(e)$ after error correction and by $I_{AE\text{total}} + (1 - I_{AE\text{total}})H_2(e/(1 - I_{AE\text{total}}))$ in privacy amplification.

The system’s optimum clock frequency was established by the measurement of $R_{sifted}$ and the error rate at different clock frequencies, and $R_{\text{net}}$ was estimated following Eq. (4). The experiment was carried out at night to eliminate the influence of the solar background radiation on the QBER. $R_{sifted}$ is directly proportional to the clock frequency as more pulses containing photons are emitted. However, the QBER increases with clock frequency due to intersymbol interference, i.e., more photons are detected in incorrect time windows. This is due to the combined timing jitter of the whole QKD system, though the maximum contribution is caused by the detectors—typically the timing jitter of the detectors ranges between 600 ps and 1 ns [28], whereas the timing jitter of the emitter and the timestamp card combined was less than 200 ps. $R_{\text{net}}$ increases with clock frequency for low values of the QBER, since the effect of higher $R_{sifted}$ is dominant. However, for higher error rates, $R_{\text{net}}$ starts to decay as more bits need to be discarded than those gained from $R_{sifted}$. From Fig. 2 it can be seen that the optimum clock frequency which provides the highest $R_{\text{net}}$ is 1.5 GHz.
with a QBER of 2.17% and an $R_{\text{net}}$ of 0.93 Mbps. All the following experiments were clocked at 1.5 GHz.

As Eq. (3) shows, $p_{\text{exp}}$ increases linearly with the channel and receiver’s transmittance $\eta$, reaching $\Delta$ rapidly unity, which means no untagged bits are left to generate a secret key. Therefore, to enhance the number of untagged bits, $\eta$ needs to be as high as possible and $\mu$ ideally should be chosen roughly proportional to $\eta$. Measurements were made to establish the QBER and $R_{\text{net}}$ for different values of $\mu$ at a fixed clock frequency of 1.5 GHz. Decreasing $\mu$ decreases the probability (given by Poisson distribution) of finding more than one photon in a nonempty pulse, and therefore, the information gained by Eve in the case of a PNS attack taking place ($I_{\text{AE/PNS}}$). However, it also decreases the detected photon rate at Bob, i.e., $R_{\text{sifted}}$. Hence there is a trade-off between security and bit rate. As Fig. 4 shows, the highest $R_{\text{net}}$ was obtained for an optimum mean photon number of 0.1 photons per pulse.

The influence of the background due to solar radiation on the performance of the system was also characterized by measuring the QBER, $R_{\text{net}}$, and the background rate (Fig. 5). The experiment was carried out under bright sunny conditions (July 31th 2012: sunset starting at 21:30). The increase of the solar background from 19:00 to 21:00 is due to straight incidence of solar rays hitting the emitter, which kept the QBER high for this period. From then on, background and QBER decrease coinciding with the sunset, and the secret key rate $R_{\text{net}}$ then reaches its maximum at 1.04 Mbps. Before sunset, a mean secure key rate of 0.62 Mbps in full bright solar conditions was demonstrated.

The stability of the link was also tested. The QBER and $R_{\text{sifted}}$ were measured every 30 min for a continuous period of 24 h under similar conditions to the previous experiments (24th of July), and the $R_{\text{net}}$ was inferred for each measurement using Eq. (4). The QBER and $R_{\text{net}}$ are represented in Fig. 6. It shows that the system runs continuously for 24 h without human interaction with a QBER between 2% and 7.8%. The maximum measured secure key rate was 1.01 Mbps, the minimum was 4.5 kbps, and the average value throughout the whole day was 0.5 Mbps. The system’s performance proves very stable, with $R_{\text{sifted}}$ and $R_{\text{net}}$ reaching 87% and 80%, respectively, of their initial values from the previous day when the experiment started. The drop in $R_{\text{net}}$ was due to a higher background (caused by slightly different weather conditions) and hence higher QBER.

The resistance of the system to vibrations and other sources of misalignment was tested by purposely misaligning the emitter from the receiver
Fig. 7. Quantum bit error rate (left-hand axis) and secure key rate $R_{\text{net}}$ (right-hand axis) against a misalignment intentionally caused at the emitter. The misalignment is calculated from the decrease in sifted bit rate at the receiver as a percentage from its optimum value, which corresponds to the system being perfectly aligned and operating at its optimum frequency (1.5 GHz) for a distance of 300 m.

from an optimized alignment at an established transmission at 1.5 GHz. Figure 7 shows that it was only after 90% of misalignment (this means that Bob has lost 90% of the initial $R_{\text{sifted}}$ when the system is perfectly aligned) that the QBER reached values higher than 6%.

Relative pointing deviations, mainly due to building sway and thermal fluctuations, were measured to cause a decrease in the sifted bit rate of 13.4% after a 24 h period. The misalignment between emitter and receiver, measured as a percentage of Bob's sifted bit rate, was characterized in Fig. 7, which shows that it is only after a misalignment of at least 60% that the QBER increases slightly (0.3%) and after 70% that this increase is more noticeable. This tendency shows that the system could potentially be aligned for 4 or 5 days without external intervention at this distance. Nevertheless, since emitter and receiver are mounted on precise gimbal platforms for their alignment, a tracking process with high-precision motors will be implemented so that in future experiments such effects can be compensated for.

Although the QKD system presented in this paper has only been experimentally tested for a 300 m link, it has been designed to withstand longer distances. Considering the attenuation on the atmospheric channel with the same urban aerosol conditions of this work (0.62 transmittance at a wavelength of 850 nm) and a regime of intermediate turbulence (refractive index structure constant $C_n^2 \approx 10^{-15}$), our simulations showed that the system could potentially operate up to a distance of 4.5 km, with a secret key rate at night of 18 kbps. For high turbulence regime ($C_n^2 \approx 10^{-14}$) the distance drops to 3.4 km.

Regarding the transmission speed of the QKD system, the maximum secret key rate $R_{\text{net}}$ (1.04 Mbps) is more than 1 order of magnitude higher than those of other systems operating at the same range of distances [8,13], and the corresponding $R_{\text{sifted}}$ (1.8 Mbps) more than 4 times the highest value reported to date for field experiments [19].

4. Conclusions and Future Work

A high-bit-rate free-space QKD system for urban applications has been reported. The modulation of high-bandwidth laser diodes with a fast frequency generator in Alice in conjunction with a synchronization at a different wavelength permits 1 order of magnitude faster key generation than those previously achieved. Spatial and spectral filtering of the background radiation, together with light-tight shielding of emitter and receiver, enables full bright daylight operation with average secret key rates reaching 0.5 Mbps. At nighttime conditions secure key rates of up to 1.04 Mbps were achieved. The stability of the system was also tested during a 24 h experiment without human interaction, and after this period the sifted and secret key rates obtained were 87% and 80% of the initial values.

The system is currently being upgraded to implement active pointing and tracking, thus permitting continuous operation.

We would like to thank José Antonio Méndez Morales for his useful advice and support, and Juan Carlos García-Gil Gallego from the Institute of Agricultural Sciences from the Spanish National Research Council (CSIC) for letting us use their facilities. We would also like to thank Jesús Martínez Mateo for fruitful discussions. We thank the Ministerio de Educación y Ciencia, projects MTM2008-02194 and 2009501073.

References


