Adaptive real time selection for quantum key distribution in lossy and turbulent free-space channels

Giuseppe Vallone,[1] Davide G. Marangon,[1] Matteo Canale,[1] Ilaria Savorgnan,[1] Davide Bacco,[1] Mauro Barbieri,[2] Simon Calimani,[1] Cesare Barbieri,[2] Nicola Laurenti,[1] and Paolo Villoresi[1,*]

[1]*Department of Information Engineering, University of Padova, via Gradenigo 6/B, 35131 Padova, Italy*

[2]*Department of Physics and Astronomy, University of Padova, vicolo dell'Osservatorio 3, 35122 Padova, Italy*

(Received 7 January 2015; published 14 April 2015)

The unconditional security in the creation of cryptographic keys obtained by quantum key distribution (QKD) protocols will induce a quantum leap in free-space communication privacy in the same way that we are beginning to realize secure optical fiber connections. However, free-space channels, in particular those with long links and the presence of atmospheric turbulence, are affected by losses, fluctuating transmissivity, and background light that impair the conditions for secure QKD. Here we introduce a method to contrast the atmospheric turbulence in QKD experiments. Our adaptive real time selection (ARTS) technique at the receiver is based on the selection of the intervals with higher channel transmissivity. We demonstrate, using data from the Canary Island 143-km free-space link, that conditions with unacceptable average quantum bit error rate which would prevent the generation of a secure key can be used once parsed according to the instantaneous scintillation using the ARTS technique.

DOI: 10.1103/PhysRevA.91.042320 PACS number(s): 03.67.Dd, 03.67.Hk, 42.50.Ex, 42.68.Bz

I. INTRODUCTION

The transmissions of quantum states to a distant receiver, which may be placed on a mobile terminal or on board of an orbiting station, is the frontier of quantum communications (QC) and of QC protocols that are based on the transmission and detection of quantum bits, or qubits. As such, it has been investigated by different groups [1–4] as well as included in continental road maps for technology development, as in the case of Europe [5], Japan [6], or China [7].

In free-space communications, background photons and detector noise are unavoidable sources of quantum bit error rate (QBER), which limits the range of quantum protocols. Indeed, in the case of quantum key distribution (QKD), an unconditional secret key may be generated only if the QBER is below a given threshold. For this reason, free-space QKD demonstrations have so far been realized typically during dark nights or by using very narrow spectral filters that impose a low key rate already on urban scale [8–17]. To overcome this limitation, a modeling of the probability distribution for the transmission coefficient was exploited, in order to devise a postselection technique for slowly fluctuating channels [18,19]. The restriction to the analysis of the sifted bit rate on a millisecond time scale was inspired by this approach [20]. However, in the case of strong turbulence, due to the inherent high losses the channel transmissivity cannot be reliably estimated in the intrinsic time scale of its variation by the received photons.

A different approach is found in the CAD1 and CAD2 distillation schemes [21], which represent a generalization of Maurer's advantage distillation technique [22]. Sequences of correct (possibly nonconsecutive) sifted bits are joined together and one single secure bit is distilled out of each sequence. The length of each sequence should be chosen according to a trade-off scheme, because longer sequences allow one to distill keys with higher channel QBERs, but provide a lower key rate in the case of low QBERs. However, in a turbulent, rapidly time-varying channel, the effectiveness of such solutions would be limited by the difficulty of choosing the suitable parameters of the distillation strategy according to the varying QBER. Another generalization of the advantage distillation in Ref. [22] was proposed in Ref. [23]: parities for many pairs of bits are shared between Alice and Bob along the public channel. Those pairs with nonmatching parities are discarded, while the remaining ones (over which the QBER is lower) are syndrome decoded. However, the above-presented distillation methods do not take advantage of the intrinsic QBER variability of the channels, as they rely on the assumption that the channel maintains its QBER stable long enough to allow optimization of their parameters.

Here, we devise a method that exploits strong atmospheric turbulence for secret key generation, in conditions in which the long-time average QBER is too high for secure communication. The temporal profile of the transmissivity in a long and strongly turbulent channel has characteristic peaks lasting few milliseconds, and following a lognormal distribution [24]. On these grounds, we will introduce and demonstrate an adaptive real time selection (ARTS) scheme, inspired by the experimental observations reported in Ref. [24], which were subsequently analyzed numerically using the split-step method in Ref. [25]. The scheme is based on the estimation of the link transmissivity over its intrinsic time scale by an auxiliary classical laser beam, copropagating with the qubits, but conveniently interleaved in time. In this way, the link scintillation is monitored in real time and the high channel transmissivity intervals corresponding to a viable QBER for a positive key generation rate can be selected. We will present a demonstration of this protocol in loss conditions that are equivalent to long distance and satellite links, and with scintillation range corresponding to moderate to severe weather.

II. EXPERIMENTAL SETUP

The 143-km free-space channel between La Palma and Tenerife Islands was used as the best available test bed for

*Author to whom correspondence should be addressed: paolo.villoresi@dei.unipd.it

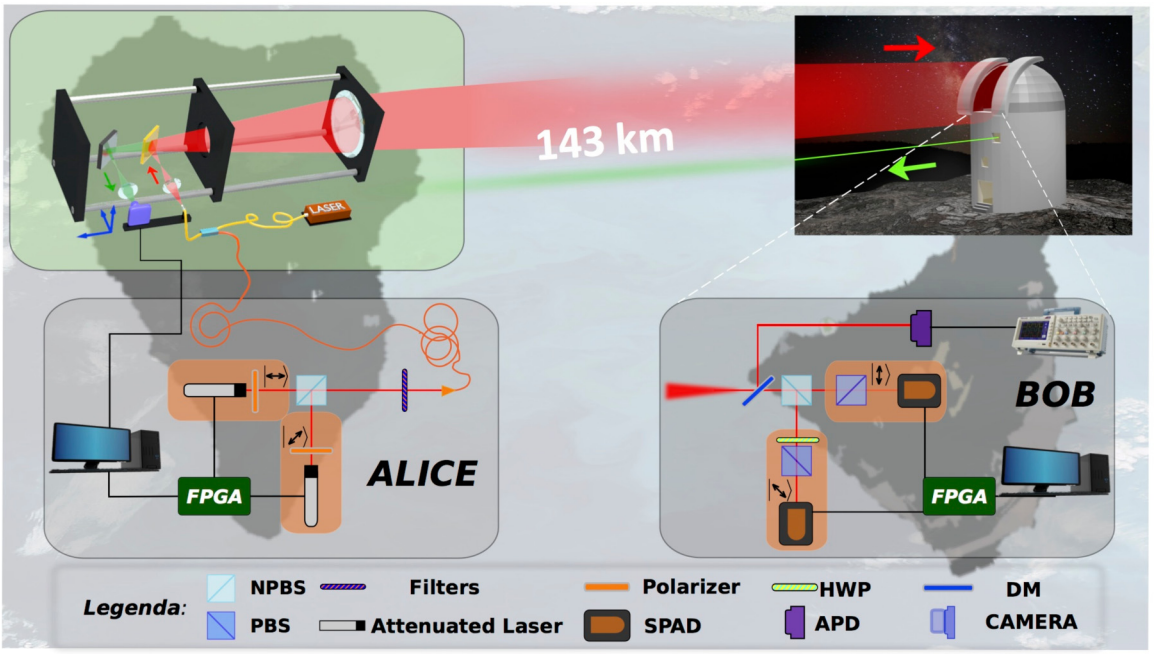

FIG. 1. (Color online) Experimental setup: Alice is located at JKT observatory in La Palma. Qubits are prepared using a field-programmable gate array (FPGA) controller, linear optical components, and attenuated lasers. Alice telescope is also configured to acquire the beacon beam sent by Bob, located at the Optical Ground Station in Tenerife, and used for tracking the transmitter in order to stabilize the pointing.

turbulence and long links, as sketched in Fig. 1. The transmitter (Alice) was located at the JKT observatory on the island of La Palma. At the transmitter side, qubits were made by using strongly attenuated 850-nm lasers. In the same location we also used a 30-mW classical laser beam (probe) at 808 nm to estimate the link transmissivity using pulses of 100 μs duration at 1 kHz repetition rate. The encoding of the quantum signal was then obtained by controlling the lasers with an FPGA. Classical and quantum beams were coupled into single mode fibers and injected into a fiber beam coupler. The output was sent to a Galilean telescope that we designed specifically with a singlet aspheric lens of 230 mm diameter and 2200 mm of focal length as the main component. The beam diameter size of about 20 cm provided the required class-1M eye-safe conditions for the free-space propagating beams. In vacuum, the telescope would produce, after 143 km of propagation, a spot comparable to the primary mirror of the receiving telescope, in order to maximize the power transfer between the two parties. To compensate the beam wandering induced by the atmosphere, we implemented a feedback loop for controlling the transmitting direction: the fiber delivering the signal to the transmitter was mounted on an XYZ movable stage placed close to the focal place of the 230-mm lens, with computer controlled stepped motors. On this same stage, we mounted a CCD sensor which acquired a green (532-nm) beacon laser sent by Tenerife toward Alice telescope. The camera is placed in order to measure an image of the singlet focal plane: the wandering of the beacon on the CCD was then analyzed in real time by a software that moves the XYZ stage to compensate the movement of the beacon spot on the camera.

At the receiver part (Bob), in Tenerife, we used the 1-m aperture telescope of the ESA Optical Ground Station to receive the signals. After the Coudé path, we collimated the beam and we divided the classical and quantum signal by using a dichroic mirror. The qubits were measured in two bases and the counts detected by the two single-photon avalanche photodiodes (SPADs) were stored on a FPGA. The probe beam is detected by a high-bandwidth avalanche photodetector and then registered and stored by an oscilloscope.

In order to measure the QBER of the channel, we used the data structure optimized for free-space QKD implementation based on a recent implementation of the B92 protocol [26,27]. A raw key is composed by N packets of 2880 bits each, sent at the rate of 2.5 MHz; as regards the payload slots, Alice sends two qubits separated by 200 ns. Due to communication constraints with the FPGA, each packet is sent every 20 ms resulting in an average sending rate of 150 kHz. The two FPGAs are synchronized every second by a pulse-per-second (pps) signal provided by two GPS receivers located in the two islands.

We point out that, at the transmitter side, the pulses contain on average more than one photon, while at the receiver side we work in the single-photon regime. Our aim, in fact, was to simulate a possible realistic scenario where one would employ fast (hundreds of MHz to GHz) free-space QKD systems which are nowadays commonly available. Since our system has a transmission rate of 2.5 MHz, the detected rate is comparable to the rate observable with a transmitter emitting true single-photon pulses with a repetition rate of about 1 GHz, assuming that the amount of optical and atmospheric attenuation is fixed.

III. REALIZATION OF THE ARTS METHOD

In order to assess the correspondence between the intensity of the probe beam and the number of photons received on the quantum channel, the link transmissivity was estimated with a fast photodiode on the probe signal. The single-photon stream

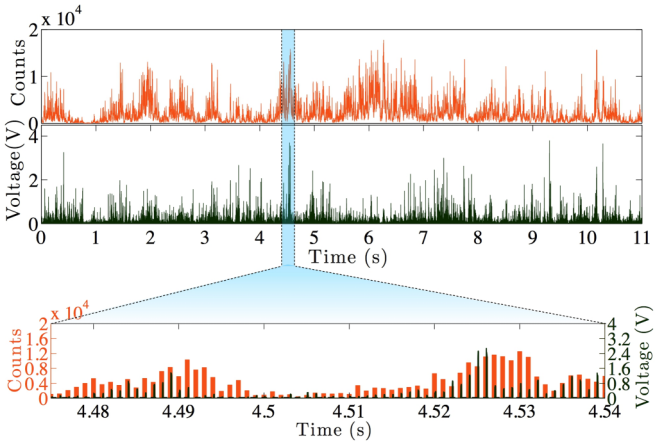

FIG. 2. (Color online) Comparison between the counts detected by the SPAD [green (dark) line] and the voltage measured by the fast photodiode at the receiver [red (light) line]. In the inset we show a zoomed detail of the acquisition (between 4.48 s and 5.54 s) in order to better appreciate the correlation between the quantum and classical signals. We chose a particular inset but in all the acquisitions the two signals are correlated.

was detected by a SPAD and binned in 1 ms intervals. With this measurement we demonstrate a good correlation between the two signals, as shown in Fig. 2 for an acquisition time of 11 s.

To further demonstrate the correlation we performed the ARTS method, consisting in the following procedure: given a set of L packets (each of 1 ms length), we denote by V_i the probe signal amplitude and by S_i the number of detected photons in the quantum signal for the ith packet. We set a threshold value V_T for the probe voltage and postselect only those packets such that $V_i > V_T$; in particular, we denote by $\mathcal{I}(V_T) = \{i : V_i > V_T\}$ the indexes of the packets for which the above condition holds and by $N_P(V_T)$ the corresponding number of packets, that is, $N_P(V_T) = |\{\mathcal{I}(V_T)\}|$. Furthermore, we define the following quantities:

$$S(V_T) = \sum_{i \in \mathcal{I}(V_T)} S_i, \quad \overline{S}(V_T) = \frac{S(V_T)}{N_P(V_T)} \tag{1}$$

with $S(V_T)$ representing the total number of detected bits and $\overline{S}(V_T)$ the mean number of detections per packet after the postselection performed with threshold V_T.

The effect of the ARTS procedure can be clearly appreciated in Fig. 3, where $\overline{S}(V_T)$ (normalized to the mean counts obtained without thresholding) is plotted (green line) as a function of the threshold: a higher threshold value corresponds to a larger mean number of counts per packet. This demonstrates that the probe and quantum signal are correlated and one can significantly improve the signal-to-noise ratio (SNR) by thresholding. Here we define the SNR as the ratio between the overall signal (true signal and background) and the background. As a side effect, we observe that the preselection also decreases the overall number of detections in the transmission $S(V_T)$ as can be noticed by considering the ratio $S(V_T)/S(V_T = 0)$ (blue line).

We then apply the results previously described to a QKD experiment. In particular, we show that, the thresholding gives,

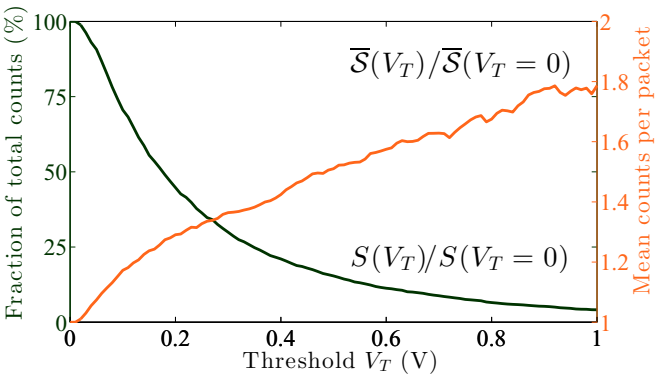

FIG. 3. (Color online) Mean counts per packet $\overline{S}(V_T)$ (normalized to the mean counts obtained without thresholding) and fraction of total count $S(V_T)/S(V_T = 0)$ in function of the probe threshold.

in some cases, benefits in terms of the secret key length, even if the total number of sifted bits decrease. Indeed, when the QBER is above the maximum value tolerable for QKD (11% for the BB84 protocol) it is not possible to produce secure keys. However, by the ARTS method we will reduce the QBER below such limit, allowing secure key generation. We point out that at the receiver the beam has a mean photon number per pulse below 1, namely, it is the single-photon level.

First, given the number of errors E_i in the ith packet, we define the overall number of errors $E(V_T)$ and the quantum bit error rate $Q(V_T)$ in the postselected packets as

$$E(V_T) = \sum_{i \in \mathcal{I}(V_T)} E_i, \quad Q(V_T) = \frac{E(V_T)}{S(V_T)}. \tag{2}$$

For evaluating the impact of the ARTS procedure on the performance of a quantum key distribution system, it is important to study the two complementary effects of thresholding: on one hand, a higher threshold increases the mean detected bits per packet $\overline{S}(V_T)$. On the other hand, it decreases the total detections $S(V_T)$. Both effects influence the achievable secret key rate of the system, and an optimal trade-off should be found.

We first derive the expected number of sifted bits and their bit error rate after thresholding. As demonstrated in Ref. [24], the statistics of the transmission of a long free-space channel follows a log-normal distribution. The measured probe voltage at the receiver, being the transmitted intensity constant, follows the same distribution, given by $p(V; m_V, \sigma^2) = \frac{1}{\sqrt{2\pi}\sigma} \frac{1}{V} \exp\{-[(\ln \frac{V}{m_V} + \frac{1}{2}\sigma^2)]^2/(2\sigma^2)\}$. In the previous expression σ^2 is related to the mean m_V and the variance v_V of the probe intensities distribution by $\sigma^2 = \ln(1 + \frac{v_V}{m_V^2})$. As an example, we show in Fig. 4 the distribution of the probabilities of occurrence of different photodiode voltages corresponding to different probe intensities as measured on the focal plane of the receiver. The shown data are the same used in Fig. 2. According to the theory [24,28], the probabilities follow a log-normal distribution, as demonstrated by the continuous (red) curve representing the log-normal fit.

In the following analysis, we assume that the number of detected photons and the probe intensity have completely correlated log-normal distributions [24]. This hypothesis

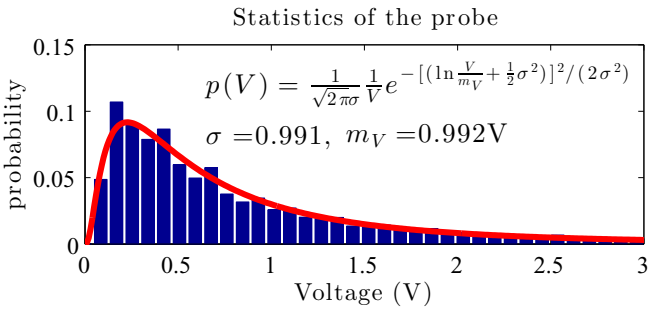

FIG. 4. (Color online) Experimental occurrences of probe intensities (measured by photodiode voltages) and log-normal fit.

implies that both distributions have the same parameter σ^2. Then, we can predict the number of packets above threshold $N_{\rm P}(V_{\rm T})$ and the number of sifted bits surviving the thresholding $S(V_{\rm T})$ in case of null background as $S(V_{\rm T})/S(0) = \int_{V_{\rm T}}^{+\infty} \frac{V}{m_V} p(V;m_V,\sigma)dV$ and $N_{\rm P}(V_{\rm T})/N_{\rm P}(0) = \int_{V_{\rm T}}^{+\infty} p(V;m_V,\sigma)dV$. By taking into account the background clicks we get

$$N_{\rm P}(V_{\rm T}) = N_{\rm P}(0)\frac{1}{2}\left[1-\mathrm{erf}\left(\frac{\ln\frac{V_{\rm T}}{m_V}+\frac{1}{2}\sigma^2}{\sqrt{2\sigma^2}}\right)\right],$$

$$S(V_{\rm T}) = n_b N_{\rm P}(V_{\rm T}) + \frac{1}{2}[S(0)-n_b N_{\rm P}(0)] \times\left[1-\mathrm{erf}\left(\frac{\ln\frac{V_{\rm T}}{m_V}-\frac{1}{2}\sigma^2}{\sqrt{2\sigma^2}}\right)\right], \quad (3)$$

where n_b is the average background count per packet. Indeed, experimental data suggest that the hypothesis of complete correlation between quantum and probe signals is not strictly satisfied, and the previous expression turns out to be an approximation of the measured values. Still, they allow one to derive a postselection threshold that improves the secure key rate, as shown in the following (e.g., in Fig. 5).

We now define a further predictive model for estimating the bit error rate on the quantum channel as a function of the probe threshold. Let us assume that the average bit error rate on the quantum channel is m_Q and that the number of counts per packet due to background noise is n_b. Now, since background photons are not polarized, the corresponding bit error rate is 1/2, and we can write the predicted quantum bit error rate $Q_{\rm th}$ as a function of the threshold $V_{\rm T}$, namely,

$$Q_{\rm th}(V_{\rm T}) = m_Q\left(1-\frac{n_b}{\bar{S}(V_{\rm T})}\right)+\frac{1}{2}\frac{n_b}{\bar{S}(V_{\rm T})}, \quad (4)$$

Given these quantities, the asymptotic key rate of a QKD system based on the BB84 protocol [29] and the ARTS procedure (namely, the probe thresholding mechanism) reads as follows:

$$R(V_{\rm T}) = \frac{S(V_{\rm T})}{S(0)}\{1-2h_2[Q(V_{\rm T})]\}. \quad (5)$$

It is worth noting that using the asymptotic rate instead of the finite-length one [30,31], may be considered a restrictive approach, especially because the postselection further reduces the number of available sifted bits. However, it is sufficient to choose the size of the blocks before key distillation (i.e., information reconciliation and privacy amplification) large enough such that, without loss of generality, the asymptotic bound provides a reasonable approximation of the actual rate.

In Fig. 5, we finally compare the theoretical (solid lines) and the experimental values (circles and crosses) of the measured QBER and the asymptotic key rate as a function of the probe intensity threshold in a data acquisition. The theoretical curves for the QBER and for the key rate were obtained by substituting in Eqs. (4) and (5) the estimates for the log-normal parameters m_V and σ^2 of the probe signal distribution. The other two parameters, $S(0)$ and $N_{\rm P}(0)$, needed for predicting $S(T)$ and $N_{\rm P}(T)$, are directly measured (they correspond to the total sifted bits and the total number of packets received, respectively).

The data shown in Fig. 5 correspond to an acquisition of 5×10^5 sifted bits in condition of high background, simulated by a thermal light source turned on in the receiver laboratory. The intensity of the background was chosen in order to obtain a mean QBER larger than 11%. In particular, we measured an average value of $n_b = 35.17$ for the background clicks per packet and we assume $m_Q = 5.6\times10^{-2}$. As clearly shown in the figure, Eq. (4) provides a good approximation of the experimental curve.

Figure 5 also shows that there is a strong correspondence between the shape of the theoretical rate, $R_{\rm th}$, and the measured rate, $R_{\rm expt.}$. The fact that the experimental points do not fit the expected curve can be ascribed to the discrepancy in the empirical joint distribution of probe intensities and counts with respect to the model; in particular, we measured the following fitting parameters for the normalized log-normal distributions: $\sigma_V^2 = 0.967$ for the probe intensities and $\sigma_S^2 = 0.716$ for the photon signal. However, the derivation of the optimal threshold for maximizing the secret key length (magenta dashed line) from the probe distribution yields the optimal $V_{\rm T}$ also for the experimental data. In particular, the optimal threshold inferred from the probe distribution is $V_{T,\rm opt}^{(\rm th)} = 375$ mV, and coincides with the one resulting from optimization on the experimental data, yielding a rate of $R(V_{T,\rm opt}^{(\rm th)}) = 5.55\times10^{-2}$.

We observe that, in the case of $V_{\rm T} < 70$ mV, it is not possible to generate a secure key, being the QBER is higher than the theoretical maximum (i.e., $Q = 11\%$). By increasing

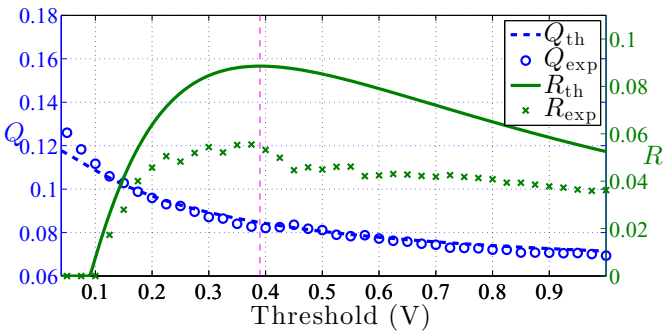

FIG. 5. (Color online) Experimental QBER ($Q_{\rm exp}$) and secure key rate ($R_{\rm exp}$) in functions of the probe threshold (measured by the photodiode voltage). Dashed and solid lines show the corresponding theoretical predictions ($Q_{\rm th}$ and $R_{\rm th}$, respectively).

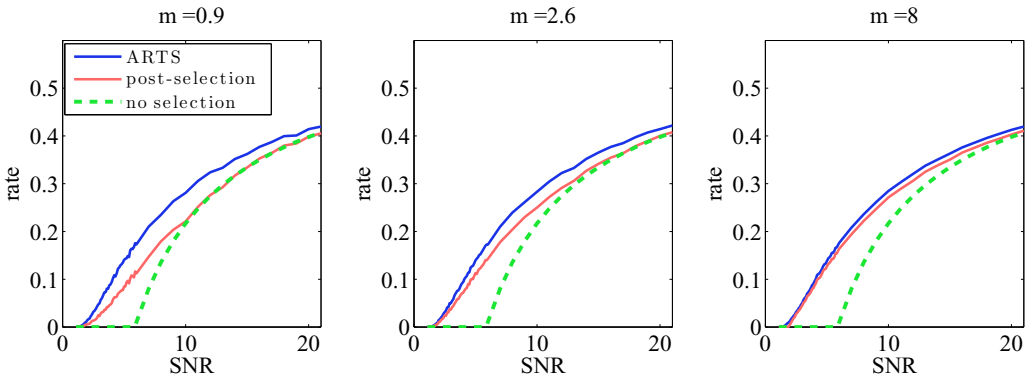

FIG. 6. (Color online) Comparison between the rates achievable by the ARTS, the postselection, and the standard QKD technique (no selection). We assumed that the channel QBER is 3% and the log-normal parameter is $\sigma = 1$, similar to the parameter we measured in the tested free-space channel. The parameter m represents the mean received bits per coherence time of the channel.

the threshold value above 70 mV a nonzero secret key rate is achieved. With the optimal threshold value, the measured QBER is $Q(V_{T,\mathrm{opt}}^{(\mathrm{th})}) = 8.38 \times 10^{-2}$; a significant improvement with respect to the initial value, $Q(0) = 13.14 \times 10^{-2}$, is therefore achieved. Finally, we observe that for increasing values of $V_{\mathrm{T}} > V_{T,\mathrm{opt}}^{(\mathrm{th})}$ the QBER still decreases, but so does the rate, since the reduction in the residual number of sifted bits does not compensate the advantage obtained from the lower QBER. This result is of absolute practical relevance, as it shows that leveraging the probe intensity information is an enabling factor for quantum key distribution, allowing one to distill a secret key.

As for the security of this postselection approach as applied to a QKD system, no advantage is given to a potential attacker in the true single-photon regime, since the thresholding is nothing but a further sifting step on the received bits [21,23]. If the attacker tried to force Alice and Bob to postselect a particular bit, in fact, she would alter the probe signal *before* the disclosure of the preparation bases on the public channel, and, therefore, before she could actually know if her measured bit is correct. On the other hand, altering the probe statistics or interrupting the probe transmission would not yield any advantage to the attacker, as it would just break the correlation between the quantum and the classical signal and would thus result in a denial of service attack. The security analysis gets more involved if we allow *photon number splitting* (PNS) attacks. In that case, the attacker may force Bob to receive just the qubits for which the PNS attack was successful, i.e., only those pulses with multiple photons. A decoy state protocol may counteract this strategy, but its effectiveness with a turbulent and loss varying free-space channel has to be investigated.

IV. COMPARISON WITH THE POSTSELECTION ON RECEIVED BITS

The ARTS method can be compared with the technique introduced in Ref. [20], where a postselection is performed when the number of received bits is above a given threshold. The postselection is effective only when the threshold is set in order to get at least several bits for coherence time of the channel: in fact, only in this condition is it possible to postselect the correct instants of high transmissivity. By coherence time of the channel we denote the time (typically of the order of few milliseconds) in which the transmissivity of the channel can be considered constant. In the case of very turbulent channel and extreme environmental conditions (say mist or high humidity), the number of received bits per channel coherence time may not exceed the value of 10: in this case, the postselection cannot be implemented and only the ARTS method remains effective. This result is confirmed by the following analysis. We performed a simulation to compare the two techniques by assuming that the probe and the signal statistics are perfectly correlated. The rates achievable in the two cases are shown in Fig. 6, demonstrating that the ARTS methods always outperform the postselection on the received sifted bits, and it is particularly effective when the number of mean sifted bits received per coherence time of the channel are below $\sim$10 and the SNR is below 20.

V. CONCLUSIONS

In conclusion, we demonstrated a proof of principle of a method that mitigates the detrimental effects of the atmospheric turbulence in QKD. The method exploits the fluctuating transmissivity of the channel for allowing QC where not possible with standard approaches. The ARTS method is easily integrable in QKD systems and is based on the sampling with a probe signal sent on the same channel of the qubits. By setting a threshold in the intensity of the probe at the receiver, it is possible to select in real time the lags of high channel transmissivity which correspond to acceptable QBER values. Indeed, we proved that with the ARTS method we were able to decrease the measured QBER and to extract secret keys in adverse conditions, when the initial average QBER is above the security threshold of 11%.

ACKNOWLEDGMENTS

The authors wish to acknowledge the help provided by Z. Sodnik of the European Space Agency and by S. Ortolani of University of Padova as well as by the Instituto de Astrofisica de Canarias (IAC), and in particular F. Sanchez-Martinez, A. Alonso, C. Warden, and J.-C. Perez Arencibia, and by the Isaac Newton Group of Telescopes

(ING), and in particular M. Balcells, C. Benn, J. Rey, A. Chopping, and M. Abreu. This work has been carried out within the Strategic-Research-Project QUINTET of the Department of Information Engineering, University of Padova and the Strategic-Research-Project QuantumFuture (STPD08ZXSJ) of the University of Padova.

[1] S. J. van Enk, J. I. Cirac, and P. Zoller, Science **279**, 205 (1998).
[2] C. H. Bennett and P. W. Shor, Science **284**, 747 (1999).
[3] H. Lo and H. F. Chau, Science **283**, 2050 (1999).
[4] R. Hughes and J. Nordholt, Science **333**, 1584 (2011).
[5] QUROPE Quantum Information Processing and Communication in Europe: http://qurope.eu/content/Roadmap and in particular http://qurope.eu/content/416-towards-long-distances-satellite-quantum-communication.
[6] NICT Quantum ICT Roadmap for Japan, available online at www.nict.go.jp/en/advanced_ict/quantum/roadmap.html
[7] H. Xin, Science **332**, 904 (2011).
[8] B. C. Jacobs and J. D. Franson, Opt. Lett. **21**, 1854 (1996).
[9] W. Buttler, R. J. Hughes, P. G. Kwiat, S. K. Lamoreaux, G. G. Luther, G. L. Morgan, J. E. Nordholt, C. G. Peterson, and C. M. Simmons, Phys. Rev. Lett. **81**, 3283 (1998).
[10] R. J. Hughes, J. E. Nordholt, D. Derkacs, and C. G. Peterson, New J. Phys. **4**, 43 (2002).
[11] J. E. Nordholt, R. J. Hughes, G. L. Morgan, C. G. Peterson, and C. C. Wipf, Proc. SPIE **4635**, 116 (2002).
[12] D. Elser, T. Bartley, B. Heim, C. Wittmann, D. Sych, and G. Leuchs, New J. Phys. **11**, 045014 (2009).
[13] M. Peev *et al.*, New J. Phys. **11**, 075001 (2009).
[14] A. Fedrizzi, R. Ursin, T. Herbst, M. Nespoli, R. Prevedel, T. Scheidl, F. Tiefenbacher, T. Jennewein, and A. Zeilinger, Nat. Phys. **5**, 389 (2009).
[15] M. García-Martínez, N. Denisenko, D. Soto, D. Arroyo, A. B. Orue, and V. Fernandez, Appl. Opt. **52**, 3311 (2013).
[16] C. Peuntinger, B. Heim, C. R. Müller, C. Gabriel, C. Marquardt, and G. Leuchs, Phys. Rev. Lett. **113**, 060502 (2014).
[17] G. Vallone, V. D'Ambrosio, A. Sponselli, S. Slussarenko, L. Marrucci, F. Sciarrino, and P. Villoresi, Phys. Rev. Lett. **113**, 060503 (2014).
[18] A. A. Semenov and W. Vogel, Phys. Rev. A **80**, 021802 (2009).
[19] A. A. Semenov and W. Vogel, Phys. Rev. A **81**, 023835 (2010).
[20] C. Erven, B. Heim, E. Meyer-Scott, J. P. Bourgoin, R. Laflamme, G. Weihs, and T. Jennewein, New J. Phys. **14**, 123018 (2012).
[21] J. Bae and A. Acín, Phys. Rev. A **75**, 012334 (2007).
[22] U. Maurer, IEEE Trans. Inf. Theor. **39**, 733 (1993).
[23] S. Watanabe, R. Matsumoto, T. Uyematsu, and Y. Kawano, Phys. Rev. A **76**, 032312 (2007).
[24] I. Capraro, A. Tomaello, A. Dall'Arche, E. Gerlin, R. Ursin, G. Vallone, and P. Villoresi, Phys. Rev. Lett. **109**, 200502 (2012).
[25] F. T. Feng Tang and B. Z. Bing Zhu, Chin. Opt. Lett. **11**, 090101 (2013).
[26] C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).
[27] M. Canale, D. Bacco, S. Calimani, F. Renna, N. Laurenti, G. Vallone, and P. Villoresi, in *Proceedings of the 4th International Symposium on Applied Sciences in Biomedical and Communication Technologies–ISABEL '11*, 1–5 (ACM Press, New York, 2011).
[28] P. W. Milonni, J. H. Carter, C. G. Peterson, and R. J. Hughes, J. Opt. B: Quantum Semiclass. Opt. **6**, S742 (2004).
[29] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing* (IEEE, New York, 1984), p. 175.
[30] D. Bacco, M. Canale, N. Laurenti, G. Vallone, and P. Villoresi, Nat. Commun. **4**, 2363 (2013).
[31] M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner, Nat. Commun. **3**, 634 (2012).