Papers in Physics, vol. 8, art. 080002 (2016)

www.papersinphysics.org

Received: 11 November 2015, Accepted: 7 January 2016
Edited by: O. Martínez
Licence: Creative Commons Attribution 3.0
DOI: http://dx.doi.org/10.4279/PIP.080002

ISSN 1852-4249

Autonomous open-source hardware apparatus for quantum key distribution

Ignacio H. López Grande,[1] Christian T. Schmiegelow,[2] Miguel A. Larotonda[1]*

We describe an autonomous, fully functional implementation of the BB84 quantum key distribution protocol using open source hardware microcontrollers for the synchronization, communication, key sifting and real-time key generation diagnostics. The quantum bits are prepared in the polarization of weak optical pulses generated with light emitting diodes, and detected using a sole single-photon counter and a temporally multiplexed scheme. The system generates a shared cryptographic key at a rate of 365 bps, with a raw quantum bit error rate of 2.7%. A detailed description of the peripheral electronics for control, driving and communication between stages is released as supplementary material. The device can be built using simple and reliable hardware and it is presented as an alternative for a practical realization of sophisticated, yet accessible quantum key distribution systems.

I. Introduction

The main goal of cryptography is to obtain a secure method to share information. This is usually achieved by the encryption of the data, using a shared cryptographic key. The security of the protocol then relies on the secrecy of this key. The distribution of a secret key is therefore a crucial task for any symmetric-key cryptographic algorithm. Classically, this can be achieved using the Diffie-Hellman method, or some variation based on it [1].

Quantum Key Distribution (QKD) protocols exploit the quantum no-cloning theorem [2] and the indistinguishability upon measurement of quantum states belonging to non-orthogonal, conjugate bases to accomplish secure distribution of cryptographic keys [3]. These features, combined with the fact that a measurement performed on a quantum system disturbs its original state in some manner, are the fundamental principles in which every QKD protocol is based on, since they allow for the detection of an eventual eavesdropper by monitoring errors on the exchanged key: the attacker cannot completely determine the measured quantum state, nor can she/he copy it; therefore she/he must resend some imperfect copy to the receiver, which may introduce errors in the key. However, a practical real-world QKD implementation is still a technical challenge that combines concepts and technologies from different areas, such as classical and quantum information theory, quantum optics, electronics and optoelectronics [4]. In this work, we describe a functional autonomous apparatus that implements the BB84 quantum key distribution protocol [5] where we implement several solutions that contribute to the affordability of a naturally costly

*E-mail: mlarotonda@citedef.gob.ar

[1] DEILAP-UNIDEF (CITEDEF-CONICET), J. B. de La Salle 4397, B1603ALO Villa Martelli, Buenos Aires, Argentina.

[2] Laboratorio de Iones y Átomos Fríos, Departamento de Física, Facultad de Ciencias Exactas y Naturales, Universidad de Buenos Aires & IFIBA-CONICET, Pabellón 1, Ciudad Universitaria, 1428 C.A.B.A., Argentina.

piece of equipment.

A critical parameter for the security of any quantum cryptography protocol is the Quantum Bit Error Rate (QBER), which is obtained after an error estimation from the sifted keys S_A and S_B —which in theory should be identical— and in the absence of an eavesdropper they are similar up to experimental errors: a small part of the key is randomly selected and used to obtain the QBER, which gives an estimation of the error rate in the whole length of the key. Once the protocol is running, the QBER is routinely monitored by resigning part of the key. It is assumed that any increase of the QBER may be generated by the presence of an eavesdropper; in such case the whole key is discarded. Theoretical upper limits have been found for the QBER rate that if preserved, unconditional security of the key can be granted [6] by applying classical error correction and privacy amplification protocols to the sifted key [7].

The first implementation of a quantum cryptographic protocol dates from 1992 [8]. Since then, the field has rapidly advanced towards sophisticated systems that provide high speed key generation [9], long distance key distribution [10, 11], transmitting photons either over optical fiber or open air, using polarization or time bin [12], or both [13], for qubit-encoding. Such protocols can be based on single photon pulses [14, 15] or on entangled photon states [19]. The use of advanced optoelectronics and high performance detectors is intensive on any QKD implementation. In this work we show that the technologies used in such quantum information algorithms are mature enough to attempt a low cost, yet functional and robust implementation of a quantum key distribution protocol. We give a detailed explanation of the communication scheme and we release the firmware code and the circuit schematics to build the control units as Supplementary Material. The following section is devoted to the description of the optical arrangements used on Alice and Bob stages. Section III. discusses the initial setup, synchronization, transmission and processing routines needed in order to generate a sifted key. The overall performance of the apparatus and its response to different perturbations are discussed thereafter.

II. Device layout

The developed system comprises an emission stage and a reception stage for the quantum channel, and an *ad-hoc* classical communication system. Quantum bits are encoded in the polarization of weak coherent pulses. These pulses are used as an approximation of a single photon pulsed source. We identify the canonical polarization states $\{|H\rangle, |V\rangle\}$ with the computational basis $B_C = \{|0\rangle, |1\rangle\}$ and the diagonal polarization states $\{|D\rangle, |A\rangle\}$ with the diagonal basis $B_D = \{|+\rangle, |-\rangle\}$. The complete scheme of the apparatus is shown in Fig. 1.

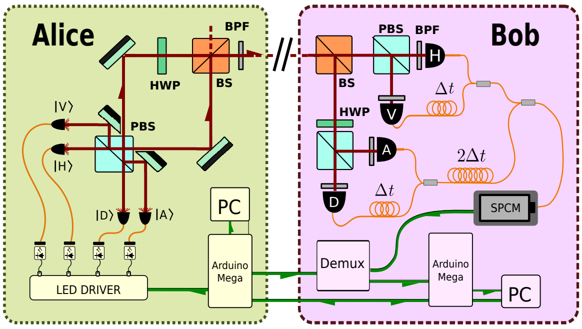

Figure 1: Setup of the QKD system: Polarization selection and spatial overlap between states is obtained with a combination of Polarizing (PBS) and non-polarizing (BS) Beam Splitters. Bob uses a BS to randomly choose the measurement basis. Polarization projections are obtained with a PBS and a half waveplate (HWP). Projected light is coupled into optical fibers and temporally multiplexed with selected delays. A single photon counting module (SPCM) is used for detection and bandpass filters (BPF) are used to reject unwanted light. Δt: 250 ns delay.

Polarized weak light pulses are generated by fast pulsing four infrared LEDs and combining them with Polarizing (PBS) and Non-Polarizing (BS) Beamsplitters: each of the LEDs is used to encode one of the four possible polarization states. The LEDs outputs are coupled and later decoupled to multimode optical fibers to define a propagation direction and divergence, and also to equalize the intensities of the four outputs. This setup is based on off-the-shelf economic infrared LEDs and avoids the use of expensive Pockel's cells and high performance HV drivers for polarization state preparation. The mean photon number per pulse was set to approximately 0.1, measured between the emission and detection stages. Assuming Poissonian photon statistics, this means that in average nearly 90% of the clock pulses carry no photons at all, while less than 0.5% of the pulses are multiphoton pulses. Both empty and multiple detection runs are considered null. It is worth to note that this particular choice of photon number per pulse does not guarantee the generation of a secure key by itself; rather, the conditions for distillation of a secure key from a raw key and the optimum photon rate depend on specific conditions of the setup, such as the length of the quantum channel –that implies distance-dependent losses–, the loss on Bob's receiver stage, and the efficiency and dark count rate of the detectors. Security conditions under different kind of attacks on non-ideal QKD systems have been reported for example in [16, 17] and reviewed in [18].

The light paths from the sources entering a polarization beam splitter (PBS) at different inputs were combined by pairs: the reflected beams exit the PBS vertically polarized, while the transmitted outputs are left horizontally polarized. A half-waveplate retarder placed in one of the outputs rotates the polarization of these two paths 45 degrees. A beam splitter cube further combines the paired sources into one common path.

Basis selection at the receiver stage is obtained using a 50% beam splitter cube to randomly obtain either a transmitted photon or a reflected photon. Projection onto the states of the canonical basis is achieved by means of a PBS, while the diagonal basis projections are obtained adding a half-wave plate retarder between the beam splitter and the PBS in one of the paths. A straightforward implementation of the detection stage demands four single photon counting modules (SPCMs), which are expensive devices. With the purpose of obtaining a practical, cost-effective setup we implemented a time multiplexed detection, adding 250 ns delays between the projection paths. The four possible measurement outcomes are encoded into temporal bins: photons are detected using only one commercial single photon counting module and labeled by the time of arrival with respect to a clock reference. Temporal demultiplexing and state determination are obtained measuring coincidences between the single photon detector output and temporal gates with selected delays. The use of a sole detector also avoids the unbalance of detection efficiencies that is present in multiple detector setups. As a drawback, this scheme presents 4 dB insertion loss per coupler, which attenuates the input signal and lowers the extractable secure key rate, due to the reduced optimal photon rate. This issue can be circumvented by implementing a decoy-state strategy together with the BB84 protocol [20–22]. Such application is currently under development at our laboratory.

The following section deals with the synchronization and control tasks performed by the open source hardware microcontrollers that allow the system to operate in an autonomous manner.

III. Control, driving and synchronization

i. Control and temporal synchronization

Open-source hardware was chosen for the processing of the cryptographic key and controlling units of the system, in order to obtain a practical, small-scale photonic implementation of the quantum protocol: all the synchronization, communication and processing operations, as well as system diagnosis were programmed on Arduino Mega 2560 microcontrollers. A diagram of the key generation protocol is sketched in Fig. 2. The communication scheme is divided in stages where classical information is exchanged (C COM) and a quantum communication stage (Q COM). An initial calibration of the system can be performed, where both parties measure the photon rate per pulse, the total temporal delay of the link and the delay between temporal bins. The communication begins with an exchange of the protocol parameters such as data structure and target key length. Then, after a synchronization sequence, they exchange the quantum bits and the sifting procedure follows: both parties exchange information on basis emission and detection and coincidences between them, keeping only the bits that come from coincident bases. The routine is repeated until the target key length is reached. The shared key is locally transferred to personal computers on each stage via USB ports.

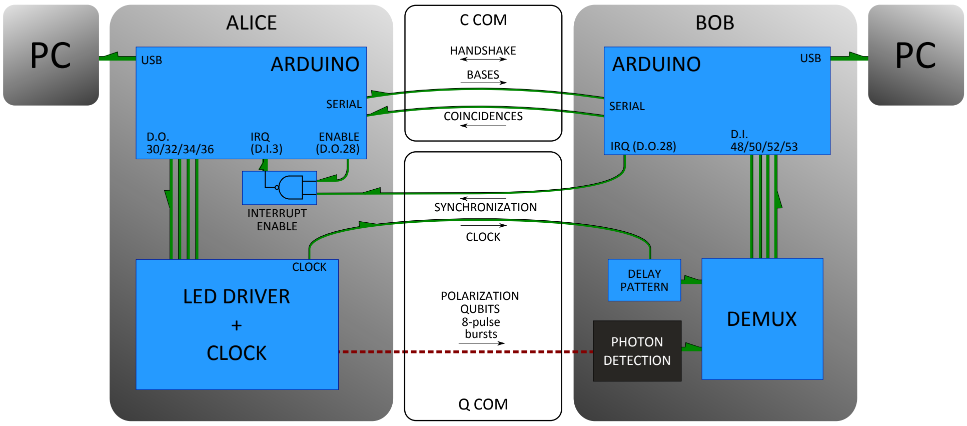

Figure 2: Communication and control setup of the BB84 QKD apparatus. The protocol is controlled by two Arduino Mega microprocessors. The synchronization start byte is generated at Bob's side and sent through an interrupt channel. After the quantum bits are sent and detected, bases are exchanged and the key is sifted. Specific input and output pins of the Arduino controllers are detailed in the figure.

ii. Electronic driving and peripherals

The communication routines described above are implemented directly by the microcontrollers. Specific tasks such as driving the pulsed LEDs, synchronizing the temporal mask and demultiplexing the temporal signals at the receiver side are performed with dedicated electronic peripherals.

Based on a random 2-bit sequence, the Arduino microcontroller sets a logic high on one of the four possible outputs. A monostable multivibrator uses this logic transition to generate a 20 ns pulse that is used as the input for a high speed LED driver. The shunt driving circuit that pulses the current on each LED is constructed using the high-current, low impedance pull-up and pull-down MOSFET transistors at the output of NAND gates and a passive network to provide a prebias current and current overshoot to increase the performance of pulsed LED drivers [23]. The optical pulse duration of 25 ns is limited by the LED response.

At Bob's side, single photon pulses are routed through different delay paths according to their polarization, and the delayed photon clicks are identified as polarization state projections by temporal demultiplexing the digital detections. Pulses from the single photon detector are addressed to the corresponding state channel by comparison with a pulse pattern that repeats the temporal delays added by the optical fibers.

IV. System performance and self-diagnostics

The main cause of bit errors are the non-ideal polarization splitting contrast of the PBSs and low quality waveplates that produce incomplete rotations and distort the ideal linear polarization states at the input and output. Also, off-the plane misalignment of the light paths within the preparation and measuring states can induce undesired rotations of the polarization axes. These are well-known problems for an open air optical setup, and workarounds to minimize them are common to any polarization-sensitive arrangement. Detector dark counts and stray light that leaks through the optical setup are also a source of error. The gated detection helps to minimize these errors. The contribution of this effect to the overall error rate depends linearly on the gate pulse duration.

The other main source of error is the temporal jitter of the signals, which can produce erroneous bit assignment of the temporally multiplexed pulses. The signal jitter is limited by the duration of the light pulse, which is approximately half the Arduino clock period. Larger pulse timing fluctuations can be produced at the generation and detection stages due to missed or added clock pulses at the microprocessors, specifically when handling interrupt signals. These temporal fluctuations can shift states from earlier to later temporal bins, inducing errors on the key. The temporal order of the multiplexed states can be arranged to minimize such errors. A natural choice is to order the detections in the sequence H (first), V, D, A (last). Such choice has an increased probability that temporal jitter can produce an error: assuming delayed detections that deterministically shift the states; in this configuration the probability of producing a bit error is 0.3125. If the delays are arranged to output the temporal sequence H (first), D, V, A (last), consecutive states at the detection pattern do not belong to the same basis. The probability of producing an error provided the states are identified in an adjacent temporal bin in this arrangement is 0.1875, and it is therefore chosen to minimize the error rate. An estimation of the bit error rate produced by this artifact in the actual protocol execution can be obtained as the product of this probability and the state-shift rate due to the overall timing jitter (0.6%), and gives approximately 1.1%. The system was tested using a mean photon rate of μ=0.09. A typical light distribution at the outputs for each polarization state generated by Alice is shown in Fig. 3a).

The apparatus autonomously generates a cryptographic key until the target key length is reached. During the tests, light pulses were emitted in bursts of 19200 pulses per second, while a constant background light of 3000 counts/s at the detector was present in the actual experimental conditions. We obtained a raw key generation rate of 363 bits/s, with a quantum bit error rate (QBER) of 2.7 %. Approximately one third of this rate (0.9 %) corresponds to errors produced by stray light and detector dark counts, while the rest of the errors are due to the electronic jitter as discussed above, and to an imperfect preparation and selection of the polarization states at the optical setup. The measured key generation rate is limited by (and it can be also estimated from) the photon-per-pulse rate, the 50% data that is discarded in average due to non-coincident bases, and the dead times on the communication stage that allow for data processing, which represents roughly two thirds of the total execution time.

During a key generation session, some parameters can be monitored for eavesdropping, inconsistencies or anomalous behavior. The sifted key can be periodically sampled and analyzed for error rate, key generation rate and bias rate (the relative abundance of "1"s to "0"s in the key, 0.98 in our setup), leading to charts like the one presented on Fig. 3b). Under normal operation conditions, the three parameters are constant through a typical one hour and a half experiment, with a relative dispersion on their average values below 2×10^{-2} for key rate, 7×10^{-3} for bit bias and 2×10^{-3} for QBER (statistics obtained over 20 kbit partitions from a total 1.9 Mbit key).

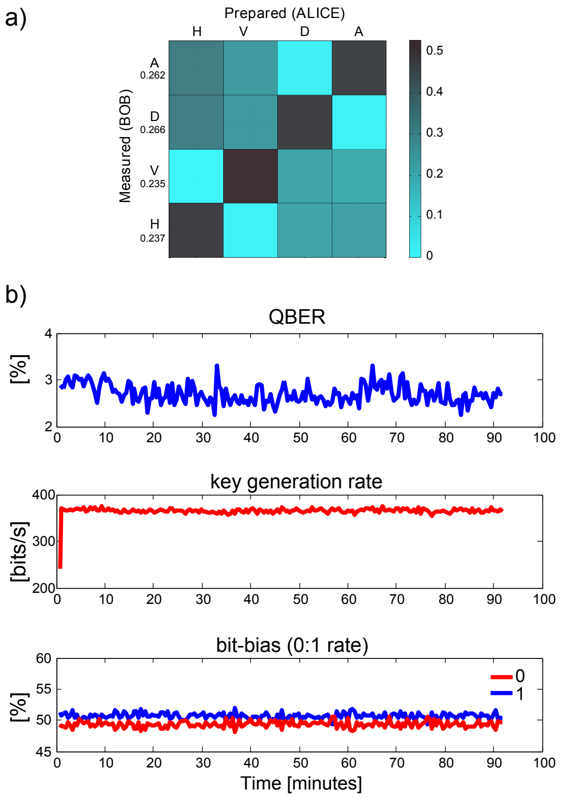

Figure 3: a) Light distribution at the detection channels, for each generated polarization state. Percentages on each row of the graph are the relative amounts of light obtained by adding the counts at each detection channel, for all the emitted states. b) Temporal evolution of different system parameters during normal operation.

The response of the system under anomalous conditions was tested disturbing the quantum channel in different manners, while the above parameters were being monitored. Figure 4 shows a sequence of such perturbations: first, in a), the detector was blocked, which caused the key rate to vanish with a characteristic time given by the integration time of the monitoring process. If one of the detection channels (V) is blocked [Fig. 4 b)], the effect is a diminished key rate and a key bias of 2/3. In c), both channels of a basis are blocked. If two channels that encode the same bit are blocked, the key rate remains at half the original rate, but now the series is completely biased, since only one logic bit is produced. More interestingly, during e), a PBS was inserted in the quantum channel, which has the following effect on the transmitted quantum states: $|H\rangle$ are left unchanged —since they are transmitted through the PBS— $|V\rangle$ states are reflected out of the path at the PBS, while $|D\rangle$ and $|A\rangle$ are transmitted as $|H\rangle$ with a 50% chance. This last feature resembles the action of an eavesdropper (Eve) using an intercept-resend strategy, where the bases in which Eve resends bits to Bob are randomly chosen. In this situation, states sent as $|V\rangle$, and (in average) half of the states originally sent on the diagonal basis, are lost at the PBS reflection, leading to a reduction of the key generation rate by a factor of two. More importantly, half of the states originally sent on the diagonal basis are transmitted through the PBS and transformed to the $|H\rangle$ state. If these states are measured on the diagonal basis, they can be detected as either $|D\rangle$ or $|A\rangle$, regardless of the original state. The result of these successive projections is that a $|D\rangle$ ($|A\rangle$) state has a non-negligible probability to be detected as a $|A\rangle$ ($|D\rangle$) state. The quantum bit error rate now raises to 25% for this particular perturbation, signaling a possible eavesdropper. The bit bias of Bob's key is 0.75: the action of the PBS that prevents all the emitted $|V\rangle$ states to be detected generates a ratio of "1"s to "0"s of 3:1. Periodically sampling and an analysis of the generated key thus provides a means for detecting intercept-resend attacks, at the cost of reducing the final key length. With the setup placed on an optical table, QBER variations as low as 0.2% can be detected.

V. Concluding remarks

We have implemented an open source hardware based autonomous QKD apparatus. Its stability and performance have been tested on megabit-length key distribution sessions, during which some key parameters were monitored. The device was designed with a cost-effectiveness approach which includes a LED-based single photon probabilistic source, a time multiplexed detection scheme that employs only one SPCM and Arduino-based controlling and processing units for Alice and Bob.

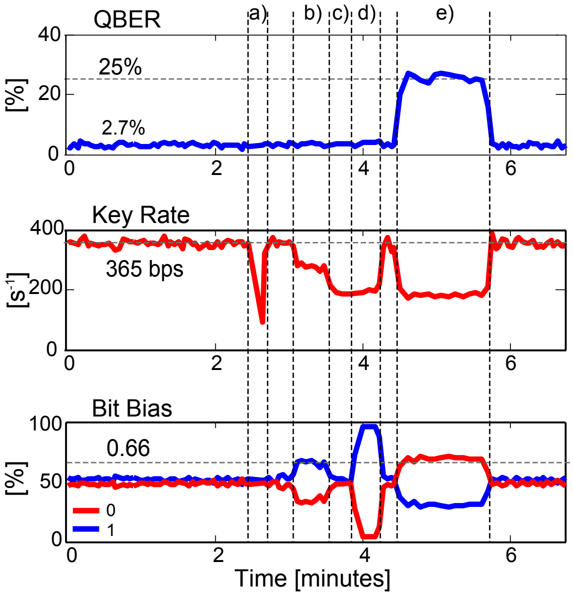

Figure 4: Behavior of the system under different perturbations on the detection stage and the quantum channel, labeled a) to e), consisting in blocking one or more detection channels and inserting a polarizing beamsplitter in the quantum channel. See the text for a detailed explanation.

The actual bit error rate can be lowered if the polarization dependent elements (PBS) on Alice and Bob sides are replaced with high-extinction ratio polarizers (at present around 1%). Another way in which the error rate can be improved is by minimizing the incidence of errors originated by detector's dark counts. This can be accomplished with a reduction on the light pulse width that leads to narrower temporal gates. Also, an increase of the mean photon number per pulse can reduce the QBER without compromising security, provided a decoy state protocol is implemented instead.

The overall protocol speed can be raised by replacing the Arduino microcontrollers with faster FPGA-based boards, where the communication and the processing blocks may be parallelized. Also, as mentioned above, the temporal demultiplexing can be done directly on the board. Faster clock boards allow for an additional reduction of the temporal delays between channels on the time multiplexed detection scheme. These can be set to be as short as 50 ns, depending on pulse width and temporal jitter.

The developed apparatus is able to autonomously generate a cryptographic key with limited yet simply improvable performance. The whole system can be used to establish a small-scale secure information channel between eye of sight distance sites, for academic purposes, or it can serve as a testbed for different quantum information-related resources, such as original protocols, detectors, light sources, or the development of alternative physical quantum channels. We understand that a cryptographic system based on well-known, simple and available technology that can be fully mastered and controlled by the end user may turn out more useful and secure than a sophisticated, "black box" type system that has many parts that are beyond the user's control, and which may depend on third party services to be operated or maintained.

Acknowledgements - This work was supported by the ANPCyT PICT 2010-2483 and MINDEF PIDDEF 012/11 grants. M.A.L. is a CONICET fellow, C.T.S. and I.H.L.G. were funded by CONICET scholarships.

[1] W Diffie, M Hellman, *New directions in cryptography,* IEEE T Inform. Theory **22**, 644 (1976).

[2] W K Wootters, W H Zurek, *A single quantum cannot be cloned,* Nature **299**, 802 (1982).

[3] M Planat, H C Rosu, S Perrine, *A survey of finite algebraic geometrical structures underlying mutually unbiased quantum measurements,* Found. Phys. **36**, 1662 (2006).

[4] N Gisin, G Ribordy, W Tittel, H Zbinden, *Quantum cryptography,* Rev. Mod. Phys. **74**, 145 (2002).

[5] C H Bennett, G Brassard, *Quantum cryptography: Public key distribution and coin tossing,* Theor. Comput. Sci. **560**, 7 (2014).

[6] N J Cerf, M Bourennane, A Karlsson, N Gisin, *Security of quantum key distribution using d-level systems,* Phys. Rev. Lett. **88**, 127902 (2002).

[7] C H Bennett, G Brassard, C Crépeau, U M Maurer, *Generalized privacy amplification,* IEEE T Inform. Theory **41**, 1915 (1995).

[8] C H Bennett *et al.*, *Experimental quantum cryptography,* J. Cryptol. **5**, 3 (1992).

[9] A R Dixon *et al.*, *Gigahertz decoy quantum key distribution with 1 mbit/s secure key rate,* Opt. Express **16**, 18790 (2008).

[10] P A Hiskett *et al.*, *Long-distance quantum key distribution in optical fibre,* New J. Phys. **8**, 193 (2006).

[11] R Ursin *et al.*, *Entanglement-based quantum communication over 144 km,* Nat. Phys. **3** 481 (2007).

[12] I Marcikic *et al.*, *Distribution of time-bin entangled qubits over 50 km of optical fiber,* Phys. Rev. Lett. **93**, 180502 (2004).

[13] W T Buttler *et al.*, *Practical four-dimensional quantum key distribution without entanglement,* Quantum Inf. Comput. **12**, 1 (2012).

[14] C H Bennett, *Quantum cryptography using any two nonorthogonal states,* Phys. Rev. Lett. **68**, 3121 (1992).

[15] H Bechmann-Pasquinucci, W Tittel, *Quantum cryptography using larger alphabets,* Phys. Rev. A **61**, 062308 (2000).

[16] N Lütkenhaus, *Security against individual attacks for realistic quantum key distribution,* Phys. Rev. A **61**, 052304 (2000).

[17] A Acin *et al.*, *Device-independent security of quantum cryptography against collective attacks,* Phys. Rev. Lett. **98**, 230501 (2007).

[18] V Scarani *et al.*, *The security of practical quantum key distribution,* Rev. Mod. Phys. **81**, 1301 (2009).

[19] A K Ekert, *Quantum cryptography based on bell's theorem,* Phys. Rev. Lett. **67**, 661 (1991).

[20] W Y Hwang, *Quantum key distribution with high loss: Toward global secure communication,* Phys. Rev. Lett. **91**, 057901 (2003).

[21] Y Zhao *et al.*, *Experimental quantum key distribution with decoy states,* Phys. Rev. Lett. **96**, 070502 (2006).

[22] Z L Yuan *et al.*, *Unconditionally secure one-way quantum key distribution using decoy pulses,* Appl. Phys. Lett. **90**, 011118 (2007).

[23] Agilent Application Bulletin 78, *Low cost fiber-optic links for digital applications up to 155 MBd*, Agilent Technologies Inc. (1999).