Abstract: In counterfactual quantum key distribution (CQKD) information is transferred, in a secure way, between Alice and Bob even when no particle carrying the information is in fact transmitted between them. In this letter we fully implement the scheme for CQKD proposed in [1], demonstrating for the first time that information can be transmitted between two parties without the transmission of a carrier.

Experimental realization of counterfactual quantum cryptography

G. Brida, A. Cavanna, I.P. Degiovanni, M. Genovese, and P. Traina*

Istituto Nazionale di Ricerca Metrologica (INRIM), strada delle cacce 91, 10135 Torino, Italy

Received: 20 October 2011, Revised: 25 October 2011, Accepted: 28 October 2011
Published online: 16 January 2012

Key words: quantum information; quantum communication; quantum interferometry; quantum counterfactual effect

1. Introduction

In the last decades quantum information [2–5] has attracted the interest of researchers all over the world. The most advanced quantum information related technology is the quantum key distribution (QKD) [6, 7], already moving from laboratories to practical applications (e.g. through more secure protocols for practical QKD [8–11]) and commercialization [12]; in fact communications over more than 100 km have been achieved both in fiber [13–19] and open air [20–25].

QKD is a method for transmitting a secret key between two partners (usually named Alice and Bob) by exploiting quantum properties of light, whose most important characteristic is that the secrecy of the generated key is guaranteed by the very laws of nature, i.e. by the properties of quantum states [6, 7] preventing the noiseless cloning of quantum bits [26].

Beyond its commercial interest, QKD represents also a fruitful test bed of concepts and ideas blossoming from quantum information theory and studies on foundations of quantum mechanics [6, 7, 27–38].

In this sense a very interesting scheme was recently presented by T.-G. Noh [1], who suggested a QKD protocol (N09) where the information is transmitted, in a secure way, between Alice and Bob even when no particle carrying the information is in fact transmitted between them. In essence the scheme exploits a counterfactual measurement, for this reason it is also known as counterfactual QKD (CQKD).

The counterfactual measurement, which relies on fundamental properties of quantum mechanics, is a typical example of interaction-free measurement that detects the
state of an object without an interaction occurring between it and the measuring device. One of its most widely known application is the Elitzur-Vaidman bomb-testing problem [39], a thought experiment successfully experimentally implemented in the nineties [40].

CQKD [1] challenges the usual paradigm requiring an effective transmission of a signal carrier (usually a photon) between the two parties exchanging information and therefore represents a very important conceptual development paving the way to further studies.

In [41] a more efficient and complicated CQKD was proposed, whereas security issues of the N09 protocol were considered in [42], where it was proved its unconditional security by considering its equivalence to an entanglement distillation protocol. Very recently, a security proof for intercept-resend attacks in realistic situation (non unit detector efficiency and presence of dark counts) was provided [43].

A first attempt to realize experimentally Noh’s scheme is reported in [44]. However, this set up missed the key element of CQKD, since the photon was indeed transmitted between Alice and Bob.

In this letter we fully implement the N09 CQKD scheme, demonstrating for the first time that information can be transmitted between two parties without the transmission of an information carrier.

1 Incidentally, we notice that the N09 protocol also challenges the paradigm of the needs of non-orthogonal states for QKD; despite that this is not the first QKD protocol based on orthogonal states, see e.g. [29–31], it is the first one whose unconditional security was proved.

2. The protocol

To explain the principle of the proposed protocol, we describe an alternative version, absolutely equivalent to the original one [1], which is shown in Fig. 1a.

Alice randomly rotates the single photon polarization (which originally is to be assumed horizontal) by means of a half wave plate (HWPA), either by 0 (bit value “0”) or by π/2 (bit value “1”). Then, the photon enters one port of a 50:50 beam splitter (BS), which is the first element of a Michelson interferometer. After BS, according to the polarization, the photon is in one of the two orthogonal states:

\[ |φ_0⟩ = (|0⟩_A|H⟩_B + i|H⟩_A|0⟩_B)/√2, \]  
\[ |φ_1⟩ = (|0⟩_A|V⟩_B + i|V⟩_A|0⟩_B)/√2. \]  

The path A of the interferometer (containing an optical delay (OD) and a mirror (M)) is inside Alice’s sector, while path B reaches Bob’s one.

Bob randomly selects one of the two polarizations and detects the photon in this polarization allowing the photon in the complementary polarization to fly back to Alice’s site. This is achieved exploiting the HWBP and the polarizing beam splitter (PBS). In particular, as the PBS addresses the |V⟩ photon towards D2, while |H⟩ photon is sent towards the mirror (M), rotations of the polarization of 0 and π/2 induced by the HWBP correspond to the detection of |V⟩ and |H⟩ photon state by D2. If the photon is not detected by D2 but reflected back by the mirror’s at Bob’s site (M) it passes through the HWBP in the selected position, thus the photon gains back its original polarization state interfering with itself at BS at Alice’s site and, for a proper tuning of the optical delay OD, it deterministically exits in D0.

When Alice and Bob select complementary polarization rotations, then either the photon is transmitted by BS and detected by Bob at D2 with 50% probability (since its polarization at PBS is vertical), or it is reflected in path A. In this case the photon, after passing through the OD twice, returns to the BS and then it is reflected or transmitted with equal probability (25%). The first case leads to the clicking of D0, the second corresponds to the photon arriving at D1H or D1V detectors depending on its polarization (selected via the PBS at Alice’s site, Fig. 1a).

After the detection is completed Alice and Bob can communicate each other whether or not each of the detectors clicked. If clicked either D0 or D2, with the purpose of detecting the intervention of an eventual eavesdropper, they announce both the detected and the initial polarization state. If D1H or D1V clicks, Alice compares the initial and final polarization states; if they are consistent she does not reveal any information, otherwise she announces her result. Alice and Bob can then establish a common key by using only the events when the photon was detected at D1H or D1V (with the correct polarization).
The only apparent difference between the scheme discussed here and the original proposal in [1] is in the apparatus used by Bob to detect the photon at D2. Nonetheless the one shown in Fig. 1a accomplishes exactly the same task of the one in the original proposal [1], thus the two schemes are absolutely equivalent.

The very interesting point of this scheme is that the selection of events only at detector D1 corresponds to photons that have traveled path A, i.e. never exited Alice’s sector. Thus, the task of creating a secret key is accomplished without any photon carrying the information having been outside Alice’s laboratory.

3. Experimental setup

In our experimental setup (Fig. 1b), equivalent to the one of Fig. 1a but with a Mach-Zehnder interferometer, a heralded single photon source exploiting parametric down-conversion (PDC) is used: a 100-mW laser emitting at 406 nm in continuous-wave regime pumps a type-I $\beta$-BaB$_2$O$_4$ (BBO) crystal producing degenerate PDC at 812 nm. The emission of the PDC photons is slightly non-collinear corresponding to an emission angle of approximately $3^\circ$ with respect to the pump direction. The heralding photon after passing through a 10 nm bandwidth interferential filter and a 4 mm wide pinhole is coupled to a multi-mode fiber and addressed to the trigger detector. The heralded photon, to be used as our true single photon state, is selected by an interferential filter and a 4 mm wide pinhole is coupled to a single mode fiber leading to the input of the interferometer.

The latter is a balanced Mach-Zehnder interferometer (MZI) in which each arm has an adjustable trombone prism. One of the two arms is entirely included in Alice’s site, while the other contains both the quantum channel and Bob’s site, the latter being composed by a PBS between two half-wave plates (HWPB1, HWPB2) and D2 detector.

The balance of the interferometer is guaranteed by a closed-loop piezo-electric movement system, which stabilizes the position of one of the trombones regulating the length difference between the two optical paths inside the MZI with nanometric resolution.

The outputs of the interferometer, after spatial selection via 1 mm diameter-wide irises, are then coupled in multi-mode fiber with no further spectral selection. A polarizer (POL) is also placed before D1 to check the polarization of the incoming photons. All the signals (including the heralding photons and D2 clicks) are revealed by single photon avalanche detectors (SPADs) with a $\approx 60\%$ detection efficiency at 812 nm.

Coincidence and time-tag analysis of the incoming signals are performed by means of PicoQuant HydrAHarP 400 multichannel picosecond event timer. All the reported data were acquired in measurements of 20 seconds.

![Figure 2](online color at www.lphys.org) Coincidence counts between the heralding channel and each of the MZI output detectors D0, D1, and D2 in 20 seconds acquisitions as a function of the displacement of the prism balancing the interferometer when Alice and Bob use compatible sets of angles (top figure: $\{0,0\}$; bottom figure: $\{\pi/2,\pi/2\}$). For this choice of angles an interference pattern (with high visibilities) can be observed in the D0 and D1 counts and also control counts (D2) are consistent with zero as expected.

4. Results

In Fig. 2 interference fringes with high visibility can be observed in the coincidence counts between the heralding channel and each of the MZI output detectors D0 and D1 as a function of the displacement of the prism balancing the interferometer (within the coherence length of the signal, which, according to the filters used, is of the order of hundreds of $\mu$m) when Alice and Bob use compatible sets of polarization rotation angles ($\{\theta_A,\theta_B\} = \{0,0\}$ or $\{\theta_A,\theta_B\} = \{\pi/2,\pi/2\}$). It can also be noticed that for this
choice of angles the D2 counts are consistent with zero as expected. In particular, when no rotation at all is performed ((0, 0)), the maximum visibilities are (92±4)% for D0 and (96±4)% for D1, while interference gets slightly reduced for (π/2, π/2) where the visibilities for D0 and D1 are respectively (87±4)% and (91±4)%, values which, nonetheless, are sufficient for the proof of the protocol. The uncertainty on the visibilities is obtained assuming a Poissonian distribution for the coincidence counts. Fig. 3 shows the stability of the interferometer in a half-an-hour long measurement when the balance of the two optical paths is fixed.

The performances of our key distribution process are summarized in Table 1. Corresponding to the angles (0, π/2) and (π/2, 0), D1 (projecting on the proper polarization, i.e. with POL set according to the polarization state sent by Alice) and D0 counts are approximately equal, in Table 1. Corresponding to the angles (0, π/2) and (π/2, 0), D1 (projecting on the proper polarization, i.e. with POL set according to the polarization state sent by Alice) and D0 counts are approximately equal, in Table 1.

In order to characterize the communication it is necessary to estimate the quantum bit error rate (QBER). Since Bob gets an incorrect bit when D1 clicks even if he and Alice use the same angle of polarization rotations and the events related to the correct transmission are those in which D1 clicks when interference is destroyed, the QBER is

\[
QBER = \frac{P_{D1,int}}{P_{D1,int} + P_{D1,nint}}
\]

where \(P_{D1,int}\) is the probability that D1 registers a photon when Alice’s and Bob’s polarization rotations are equal, such that there is (destructive) interference, and \(P_{D1,nint}\) is the analogous probability in the case in which Alice and Bob choose different polarization angles.

For our measurements the mean QBER is QBER = (12±1)%. We underline that all the reported measurements are obtained without subtraction of background and accidental counts. If we account for these contributions, the corrected QBER value decreases noticeably to QBER'=(7±1)%, as would be the case if more reliable detectors were used, such as detectors affected by a lower dark count rate. The still large value of the corrected QBER is mainly due to the non ideal behavior of the half-wave plates (HWP1 and HWP2). As mentioned, the protocol has been demonstrated absolutely secure when ideal single photon sources are employed. To address the security problems eventually raised by the practical implementation of the protocol, firstly we tested it against possible photon-number-splitting attacks, i.e. we investigated the quality of our heralded single photon source. From the measured count rates we obtained a value of \(g^{(2)}(0) = (7±5) \times 10^{-3}\), which clearly shows negligible presence of multi-photon components.

The reason for such a small value is related to the very low level of count rates (180 maximum in 20 seconds acquisitions) at the detectors. This is due to the poor coupling efficiency of the heralded source (=5%), the strict spectral selection on the heralding photons (1 nm FWHM) and the spatial selection at the interferometers output (1 mm irises). Furthermore, a small temporal detection window (1 ns) was selected in correspondence of the arrival of the heralding photon. Because of this strong temporal post-

---

**Table 1** Resume of the main results in the implementation of the CQKD protocol proposed in [1]. Each column refers to a set \(\{\theta_1, \theta_2\}\) of polarization rotation performed by the users and \(C_{Di}\) labels the mean coincidence counts at the \(i\)-th detector in acquisition of 20 seconds. \(V_{Di}\) are the visibilities of the interference fringes observed at the two outputs of the interferometer by scanning the path length difference between the two arms of the MZI. QBER is the estimated quantum bit error rate for the transmission.

| \(\{\theta_1, \theta_2\}\) | \(C_{D0}\) | \(V_{D0}\) | \(V_{D1}\) | QBER |
|--------------------------|----------|----------|----------|------|
| (0, 0)                   | 180±4    | 59±2     | 59±2     |      |
| (0, π/2)                 | 7.9±0.9  | 53±2     | 7.2±0.9  | 59±2 |
| (π/2, π/2)               | 6.6±0.8  | 85±3     | 5.4±0.7  | 86±3 |
| (0, π)                   | (92±4)%  | (0±4)%   | (0±4)%   | (91±4)% |
| (π/2, 0)                 | (96±4)%  | (0±4)%   | (0±4)%   | (91±4)% |

---

**Figure 3** (online color at www.lphys.org) Counting events showing the stability of the interferometer in a half-an-hour long measurement when the balance of the two optical paths is fixed.
selection, unheralded photons could travel inside the channel and Eve may exploit that to get significant information by intercepting them. This security issue could be overcome by using shuttered heralded single-photon sources [45].

We also address the issue of robustness of the protocol against more general attacks by computing the difference \( m = I_{AB} - I_{AE} \), where \( I_{AB} \) and \( I_{AE} \) is the mutual information between Alice and Bob (Alice and Eve), in the cases of general Intercept-Resend attacks and “Time-Shift” attacks. Following the models suggested in [43], one can express \( m \) for the intercept-resend attack as

\[
m_{IR} = P_{D1} \left[ 1 - h \left( \frac{P_{e1}}{P_{D1}} \right) \right],
\]

where \( P_{D1}, P_e \) are respectively the click probability and the error probability at D1 and \( h(x) \) is the binary Shannon entropy. \( P_{e1} \) includes not only the probability of registering counts at D1 when they are not expected (i.e. \( \{\theta_A, \theta_B\} = \{0\} \) or \( \{\theta_A, \theta_B\} = \{\pi/2, \pi/2\} \)), but also the probability of detecting a photon at D1 with the wrong polarization. The measured rate of photons in D1 with a polarizer orthogonal to Alice’s one is \((1.3 \pm 1.2) \) counts in 20 seconds (on average over the possible polarization settings), corresponding to a \( \approx 2\% \) contribution to \( P_{e1} \), almost half of the overall \( P_{e1} \approx 4\% \).

Regarding the time-shift attack, where Eve exploits the non-ideality of the detectors, one must subtract from the previous value two contributions, obtaining:

\[
m_{TS} = m_{IR} - \gamma - \Delta I_{AE}(\eta),
\]

where \( \gamma \) accounts for the maximum corrupted bit rate due to dark counts and

\[
\Delta I_{AE}(\eta) = \frac{1}{2 \eta} (P_{e2} - P_{c2})
\]

is the increment of the mutual information between Alice and Eve due to non-unit efficiency of the detectors [46].

Both values calculated from the collected data are positive \((m_{IR} = 0.25 \pm 0.05, m_{TS} = 0.19 \pm 0.05)\), ensuring the possibility of distributing a secret key [6,7].

Altogether our results provide a satisfying proof-of-principle of the QKD scheme realized in free-space. Recent results on the implementation of high stability fiber based Mach-Zehnder interferometers (over distances of the order of some km) [47,48] certify the possibility of exploiting this protocol in “real-life” (as well as commercial) applications.

5. Conclusions

In conclusion we have presented the first experimental demonstration of counterfactual QKD. This result, beyond its eventual practical interest, has a huge conceptual significance since it demonstrates for the first time as information can be transmitted between two partners, thanks to quantum systems peculiar properties, in a situation where no carrier has been actually transmitted between them.

Our results show good agreement with the theoretical predictions and represent a proof of principle of the experimental feasibility of CQKD.

Acknowledgements: We acknowledge the support of the Joint Research Project EMRP ind-06-MIQC with funding by the European Union. The authors also thank Dr. Alessio Avella for fruitful discussion.

References

[1] T.-G. Noh, Phys. Rev. Lett. 103, 230501 (2009).
[2] D. Bouwmeester, A.K. Ekert, and A. Zeilinger (eds.), The Physics of Quantum Information: Quantum Cryptography, Quantum Teleportation, Quantum Computation (Springer, Berlin – Heidelberg – New York, 2000).
[3] M.A. Nielsen and I.L. Chung, Quantum Computation and Quantum Information, Cambridge Series on Information and the Natural Sciences (Cambridge University Press, Cambridge, 2000).
[4] D.J. Wineland and D. Leibfried, Laser Phys. Lett. 8, 175 (2011).
[5] D.V. Sych, B.A. Grishanin, and V.N. Zadkov, Laser Phys. Lett. 3, 102 (2006).
[6] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. 74, 145 (2002) and references therein.
[7] V. Scarani, H. Bechmann-Pasquinucci, N.J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys. 81, 1301 (2009) and references therein.
[8] W.-Y. Hwang, Phys. Rev. Lett. 91, 057901 (2003).
[9] V. Scarani, A. Acín, G. Ribordy, and N. Gisin, Phys. Rev. Lett. 92, 057901 (2004).
[10] Y.-C. Jeong, Y.-S. Kim, and Y.-H. Kim, Laser Phys. 21, 1438 (2011).
[11] D.A. Kronberg and S.N. Molotkov, Laser Phys. 19, 884 (2009).
[12] T. Länger and G. Lenhart, New J. Phys. 11, 055051 (2009).
[13] E. Diamanti, H. Takesue, C. Langrock, M.M. Fejer, and Y. Yamamoto, Opt. Express 14, 13073 (2006).
[14] P.A. Hiskett, D. Rosenberg, C.G. Peterson, R.J. Hughes, S. Nam, A.E. Lita, A.J. Miller, and J.E. Nordholt, New J. Phys. 8, 193 (2006).
[15] I. Marcikic, H. de Riedmatten, W. Tittel, H. Zbinden, M. Legré, and N. Gisin, Phys. Rev. Lett. 93, 180502 (2004).
[16] A. Tanaka, M. Fujiiwara, S.W. Nam, Y. Nambu, S. Takeda, W. Maeda, K. Yoshino, S. Miki, B. Baek, Z. Wang, A. Tajima, M. Sasaki, and A. Tomita, Opt. Express 16, 11354 (2008).
[17] A.R. Dixon, Z.L. Yuan, J.F. Dynes, A.W. Sharpe, and A.J. Shields, Opt. Express 16, 18790 (2008).
[18] D. Stucki, N. Walenta, F. Vannel, R.T. Thew, N. Gisin, H. Zbinden, S. Gray, C.R. Towery, and S. Ten, New J. Phys. 11, 075003 (2009).
[19] D. Rosenberg, C.G. Peterson, J.W. Harrington, P.R. Rice, N. Dallmann, K.T. Tyagi, K.P. McCabe, S. Nam, B. Baek, R.H. Hadfield, R.J. Hughes, and J.E. Nordholt, New J. Phys. 11, 045009 (2009).
[20] A.A. Semenov and W. Vogel, Phys. Rev. A 80, 021802 (2009).
[21] E. Meyer-Scott, H. Hüb el, A. Fedrizzi, C. Erven, G. Weihs, and T. Jennewein, Appl. Phys. Lett. 97, 031117 (2010).
[22] T. Schmitt-Manderbach, H. Weier, M. Fü rst, R. Ursin, F. Tiefenbacher, Th. Scheidl, J. Perdigues, Z. Sodnik, C. Kurtsiefer, J.G. Rarity, A. Zeilinger, and H. Weinfurter, Phys. Rev. Lett. 98, 010504 (2007).
[23] R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek, B. Ö mer, M. Fü rst, M. Meyenburg, J. Rarity, Z. Sodnik, C. Barbieri, H. Weinfurter, and A. Zeilinger, Nat. Phys. 3, 481 (2007).
[24] C. Bonato, A. Tomaello, V. Da Deppo, G. Naletto, and P. Villoresi, New J. Phys. 11, 045017 (2009).
[25] N. Antonietti, M. Mondin, F. Daneshgaran, G. Giovanelli, I. Kostadinov, B. Lunelli, G. Brida, M. Genovese, and M. Gramegna, Int. J. Quantum Inf. 7, 213 (2009) and references therein.
[26] M. Barbieri, F. Ferreyrol, R. Blandino, R. Tualle-Brandi, and Ph. Grangier, Laser Phys. Lett. 8, 411 (2011).
[27] M. Genovese, Phys. Rep. 413, 319 (2005) and references therein.
[28] A.K. Ekert, Phys. Rev. Lett. 67, 661 (1991).
[29] L. Goldberg and L. Vaidman, Phys. Rev. Lett. 75, 1239 (1995).
[30] L. Goldberg and L. Vaidman, Phys. Rev. Lett. 77, 3265 (1996).
[31] A. Avella, G. Brida, I.P. Degiovanni, M. Genovese, M. Gramegna, and P. Traina, Phys. Rev. A 82, 062309 (2010).
[32] K. Boström and T. Felbinger, Phys. Rev. Lett. 89, 187902 (2002).
[33] I.P. Degiovanni, I. Ru o Berchera, S. Castelletto, M.L. Rastello, F.A. Bovino, A.M. Colla, and G. Castagnoli, Phys. Rev. A 69, 032310 (2004).
[34] M. Lucamarini and S. Mancini, Phys. Rev. Lett. 94, 140501 (2005).
[35] A. Cerè, M. Lucamarini, G. Di Giuseppe, and P. Tombesi, Phys. Rev. Lett. 96, 200501 (2006).
[36] M. Lucamarini, J.S. Shaari, M.R.B. Wahiddin, arXiv:0707.3913.
[37] Y.-S. Kim, Y.-C. Jeong, and Y.-H. Kim, Laser Phys. 18, 810 (2008).
[38] F.A.A. El-Orany, M.R.B. Wahiddin, M.-A. Mat-Nor, N. Jamil, and I. Bahari, Laser Phys. 20, 1210 (2010).
[39] A.C. Elitzur and L. Vaidman, Found. Phys. 23, 987 (1993).
[40] P. Kwiat, H. Weinfurter, T. Herzog, A. Zeilinger, and M.A. Kasevich, Phys. Rev. Lett. 74, 4763 (1995).
[41] Y. Sun and Q.-Y. Wen, Phys. Rev. A 82, 052318 (2010).
[42] Z.-Q. Yin, H.-W. Li, W. Chen, Z.-F. Han, and G.-C. Guo, Phys. Rev. A 82, 042335 (2010).
[43] S. Zhang, J. Wang, C.-J. Tang, and Q. Zhang, arXiv:1103.0601.
[44] M. Ren, G. Wu, E. Wu, and H. Zeng, Laser Phys. 21, 755 (2011).
[45] G. Brida, I.P. Degiovanni, M. Genovese, A. Migdall, F. Pipacentini, S.V. Polyakov, and I. Ru o Berchera, Opt. Express 19, 1484 (2011).
[46] G. Brida, M. Genovese, and M. Gramegna, Laser Phys. Lett. 3, 115 (2006).
[47] G.B. Xavier and J.P. von der Weid, Opt. Lett. 36, 1764 (2011).
[48] G.B. Xavier, T.R. da Silva, G.P. Temporão, and J.P. von der Weid, Electron. Lett. 47, 608 (2011).