Hindawi Publishing Corporation
Advances in High Energy Physics
Volume 2012, Article ID 801982, 10 pages
doi:10.1155/2012/801982

Research Article

Perspectives on Entangled Nuclear Particle Pairs Generation and Manipulation in Quantum Communication and Cryptography Systems

Octavian Dănilă, Paul E. Sterian, and Andreea Rodica Sterian

Academic Center of Optical Engineering and Photonics, Polytechnic University of Bucharest, 313 Spl. Independentei, 060042 Bucharest, Romania

Correspondence should be addressed to Andreea Rodica Sterian, andreea.sterian1@yahoo.com

Received 30 September 2012; Accepted 29 October 2012

Academic Editor: Bogdan Mitrica

Copyright © 2012 Octavian Dănilă et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Entanglement between two quantum elements is a phenomenon which presents a broad application spectrum, being used largely in quantum cryptography schemes and in physical characterisation of the universe. Commonly known entangled states have been obtained with photons and electrons, but other quantum elements such as quarks, leptons, and neutrinos have shown their informational potential. In this paper, we present the perspective of exploiting the phenomenon of entanglement that appears in nuclear particle interactions as a resource for quantum key distribution protocols.

1. Introduction

Quantum entanglement has long been proven to be the most resourceful method of achieving feasible, high fidelity quantum key distribution over growing distances [1–6]. Exploiting entanglement can be done using multiple observables, giving experiments a practical versatility. Polarization entangled states [7], while being very easily obtainable, are very hard to manipulate as they propagate through different media such as optical fibers. On the other hand, time-bin entanglement is harder to obtain, but manipulation requirements, such as temperature, polarization, and propagation velocity, are easier to fulfill. Quantum key distribution [8, 9] schemes that have been applied to regular qubits may be applied to qubits that result from nuclear interactions. The conventional method of achieving quantum key distribution is generating quantum elements photons and manipulating them as such as to obtain the desired states on which quantum key distribution operates. To this extent, quantum key distribution can be obtained using either single or entangled states, and due to the nature of the two, there have been devised two different protocols that extract the information from the generated states. The first protocol [8], created by Charles Bennett and Gilles Brassard—BB84 employed singular photonic states, with no coherence between their informational values. The information-carrying observable was the polarization of the photon, on which the two participants carry out local operations, that is, rotations in the analysis vector bases and classical communication in which the two participants communicate a part of their informational operators either the values obtained or the analysis bases in which the single states are detected. The second protocol [9], elaborated by Artur Ekert—Ek91, is derived from the BB84 protocol but differs from it in an essential manner: it employs bidimensional, maximally entangled states, also called Bell states. The usage of entangled states has major advantages, and the source that supplies the participants need not be a part of the particular setup of the transmitter. Thus, participants can share random keys supplied by a dedicated encryption server. Any quantum key distribution protocol makes interceptor detection possible, by verification of the qubit error rate that any foreign measurement induces onto the states prepared by the two participants. The qubit error rate is calculated either by direct verification of the raw keys obtained after single state communication or by carrying out standard Bell measurements, in order to establish entanglement quality after key communication. Optimal attacks [9] which are the most efficient in the present days induce an error rate of approximately 15%. Thus if after key distribution the two participants have two keys that differ with more than 15%, they drop the conversation on the count that an interceptor was found on the channel.

In practical setups, entangled states are considered to be favorable to single states, simply by not requiring any participant to employ costly equipment on this setup. A big disadvantage, however, is that because of the no-cloning theorem, the created entangled states cannot be reproduced. While entanglement does not decay naturally, depolarization and thermal interaction are liable to destroy the created state over long communication distances. Secure quantum key distribution was achieved over a distance of several kilometers in a single-mode optical fiber [10–12], and although promising, long-distance communication may just be too much for conventional photon pair entangled state communications. To overcome this obstacle, one may consider using other information carriers that have better propagation performances than photons. The best candidate for this task is the neutrino, known for the fact that it travels through any medium without any absorption, making long-distance communication a very feasible idea. The goal of this paper is to highlight the perspective of using entangled nuclear pairs in quantum key distribution protocols. The paper is structured as follows. Section 2 covers the theoretical background of entangled states and quantum key distribution protocols, Section 3 presents the experimental setup for entangled photon pairs, and Section 4 treats the perspective of employing nuclear particles as entangled states. Finally, conclusions are drawn in Section 5.

2. Theoretical Background

The quantum description of nature has been developed as a consequence of Gedanken experiments [13], which revealed that quantum elements exhibit a dual behaviour of particle and wave, which can be projected into the desired state depending on the type of measurement carried out. The main advantage of quantum states is that for any orthogonal basis $|0\rangle$ and $|1\rangle$, all quantum states can be described as a superposition of the two, as $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$. The probability amplitudes α and β satisfy the relation $|\alpha|^2 + |\beta|^2 = 1$—the normalization equation. In the bidimensional case, representation of the compound state is written as $|\varphi\rangle = |\psi\rangle \otimes |\psi\rangle = |\psi\psi\rangle$. Any compound state that can be factorized into the compounds is called a separable state. However, some physical interactions between quantum elements yield states of the form [7]

$$\begin{aligned} |\psi\rangle^{\pm} &= \alpha|01\rangle \pm \beta|10\rangle, \\ |\phi\rangle^{\pm} &= \alpha|00\rangle \pm \beta|11\rangle, \end{aligned} \tag{2.1}$$

which cannot be decomposed into their compounds. These are formally defined as entangled states. Correlations between the states hold for any distance between the quantum elements, and for their entire lifetime should no external destructive interaction occur. For $\alpha = \beta = 1/\sqrt{2}$, maximally entangled or Bell states can be obtained.

Discerning between separable and entangled states is an important prerequisite for applications. The most general method employed is the verification of Bell's inequality [10, 11]. It has been shown that all separable states respect the relation

$$E(a,b) + E(b,c) + E(c,d) - E(d,a) < 2 \tag{2.2}$$

with $E(x,y)$ being the experiment of measuring the informational values of two systems given by variables x and y, with results $E(x,y) = \pm 1$. Entangled states violate this inequality, yielding

$$E(a,b) + E(b,c) + E(c,d) - E(d,a) = 2\sqrt{2} \tag{2.3}$$

for maximally entangled or Bell states.

Quantum key distribution protocols use quantum states in order to produce naturally and purely random keys that can further be applied into cryptographic schemes such as the Vernam protocol. In addition to this, any eavesdropper that listens in on the communication will leave a trace in the transmitted keys in the form of qubit error rate, should this rate be greater than 15%. As seen in Figure 1, the Ekert protocol consists of an entangled photon pair source that sends maximally entangled states to both participants (called Alice and Bob). They choose to analyse the incoming photons on three conventional angles—22.5°, 45°, and 67.5°. Alice uses 22.5° and 45°, while Bob uses 45° and 67.5°. The common polarization angle is set to detect the raw key that will be used for encryption, while the other two angles are used for verification of Bell's inequality. Depending on the type of entangled states the source supplies, Alice and Bob will ideally obtain either identical or complementary raw keys. The quality of entanglement can be calculated by randomly selecting states measured on the 22.5° and 67.5° analysis angles and calculating the Bell inequality. Eavesdropping on the protocol induces a degradation of entanglement, up to a point that the conversation is dropped.

Generation of entangled states is achieved through different methods for different quantum elements. In the case of photons, generation of polarization-entangled photons is achieved either by spontaneous parametric downconversion (SPDC), which occurs in second-order nonlinear optical media, or by quantum dot experiments. In the case of SPDC,

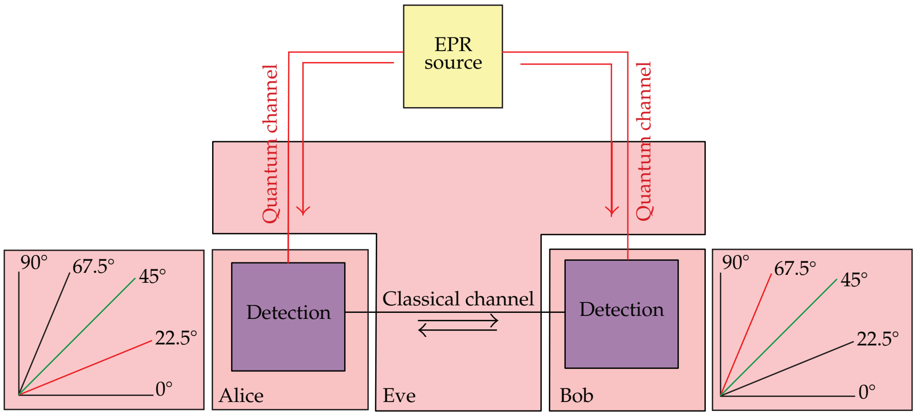

Figure 1: Scheme of the Ek91 protocol.

one pump photon instantly converts into two polarization entangled photons that respect the energy and momentum conservation laws [14, 15]:

$$\begin{gathered} \omega_p = \omega_s + \omega_i, \\ \overline{k}_p = \overline{k}_s + \overline{k}_i, \end{gathered} \tag{2.4}$$

where indices p, s, and i denote the pump, signal, and idler photons. Efficiency of entangled state generation ranges from 10^{-12} to 10^{-7}, which leads to a good entangled photon pair rate for pump powers of hundreds of milliwatts. Naturally, the conservation laws hold for fixed frequencies that are almost impossible to maintain constant. This effect is called phase matching. In some nonlinear optical media, the nonlinear optical susceptibility has its sign changed in some regions, which leads to the creation of a locally characteristic wavenumber K that fulfills the relation:

$$\overline{k}_p = \overline{k}_s + \overline{k}_i + \overline{K}. \tag{2.5}$$

Thus, as seen in Figure 2, depending on constructive parameters, the desired phase matching considerations can be achieved.

3. Entangled Photon Pair Source Experiment

Having all the previous considerations, entangled photon pair sources that offer up to 1100 pairs/s have been constructed [16–22], with competitive operational parameters. Raw and net visibilities of 97% and 99.5%, respectively, have been obtained, with a Bell parameter of 2.8. The full source setup is illustrated in Figure 3. The layout of the source consists of a 2-Watt Ti : Sa laser pumping a 3.5 cm long, periodically poled lithium niobate waveguide with a 6 μm poling period, obtaining a type II entangled photon pair with 10^{-9} efficiency. The generated pair was then transmitted through standard telecom fiber devices to the detection module, where two ultramodern InGaAs avalanche photodiodes, running in gated mode, register the coincidences [23–26].

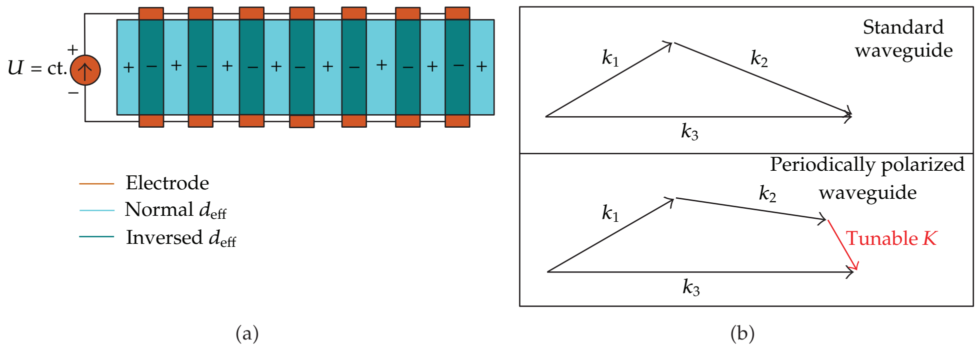

Figure 2: Entangled photon pair generation devices: (a) periodically poled waveguide structure; (b) phase matching and quasiphase matching for waveguides.

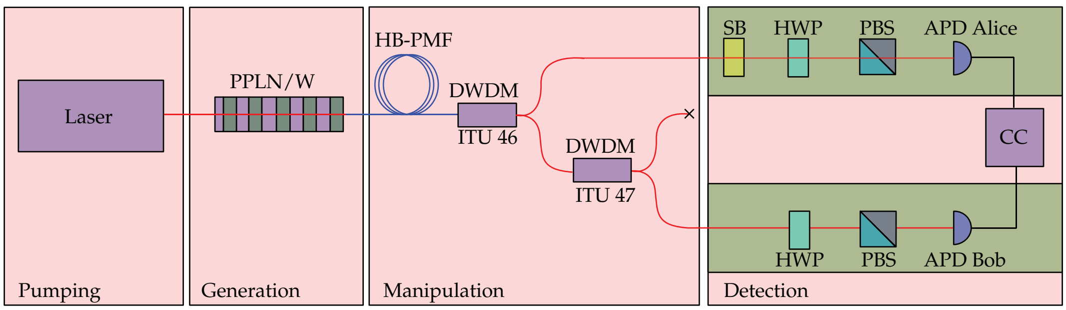

Figure 3: Layout of the source.

In order to successfully transmit the generated entangled state, the signal and idler photons have to be identical for any other measurement except polarization; otherwise the state is inherently destroyed. Manipulation of the photons has been carried out by means of spectral and temporal overlapping. Spectrum overlapping has been achieved by stabilizing the waveguide temperature up to 0.1°C. The spectrums have been filtered using two adjacently centered ITU channels dense width division multiplexers, that ensure that, if a photon is detected in one filter window, the other one is sure to be found in the complementary one. Thus, deterministic postselection of photons has been obtained as is shown in Figure 4(a). Temporal overlapping has been obtained by employing a simple high-birefringence polarization maintaining optical fiber that is used to compensate for the delay between the two different velocities of the photons in the waveguide. This solution is illustrated in Figures 4(b) and 4(c).

The detection modules are standard Bell measurement arrangements that consist of a half waveplate, a polarized beam splitter and an avalanche photodiode at each side, and a Soleil Babinet phase compensator placed at one of the two modules. The two photodiodes operate in gated mode, in order to minimize dark counts as follows: when Alice's photodiode records a photon, it commands Bob's photodiode to open, over a series of electronic equipment. Bob's side has a delay line after the polarized beam splitter long enough that the photon that propagates through it spends just as much time needed for the open command signal to reach Bob's photodiode. The Bell measurements conducted are carried out by forcing Alice to fix her analysis basis and then varying the analysis angle on Bob's side.

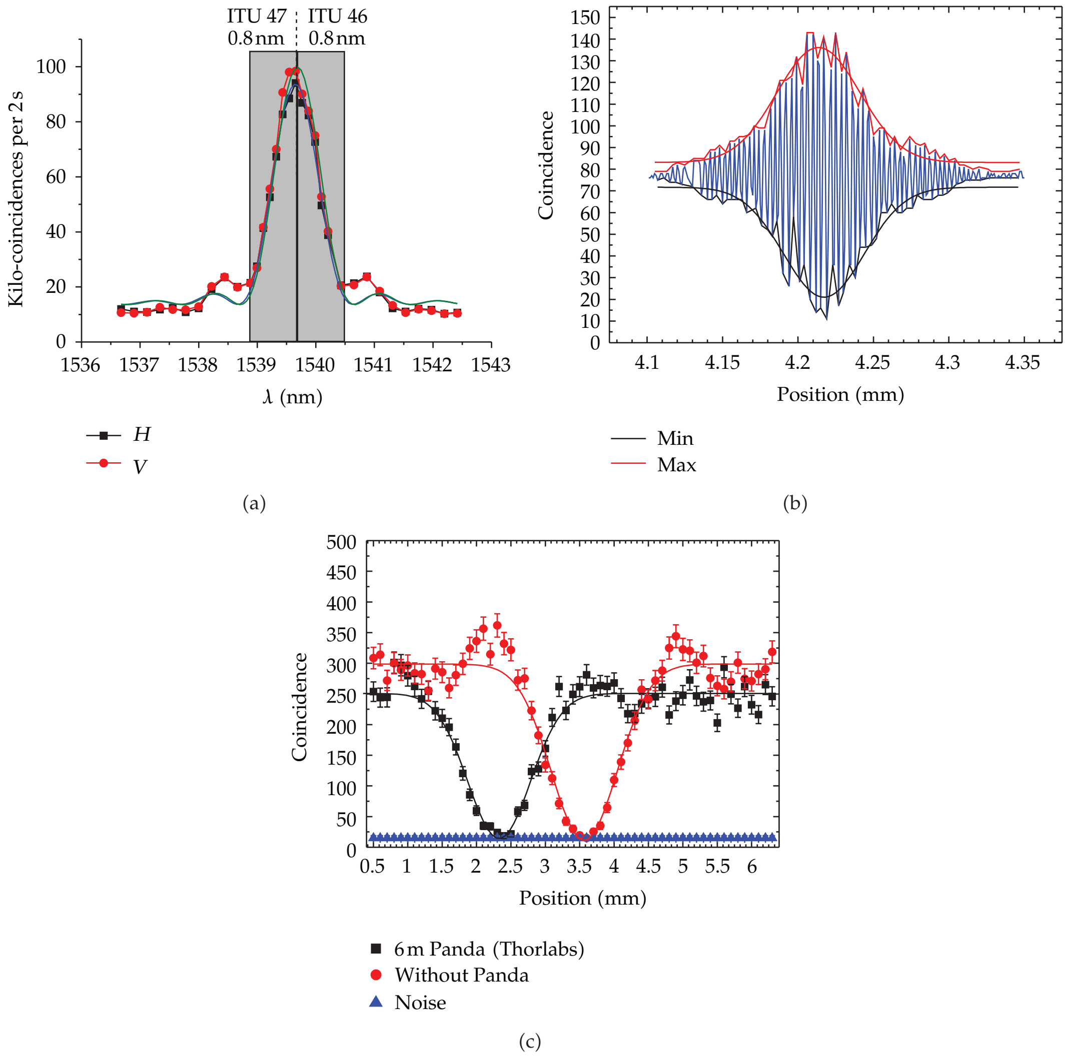

Figure 4: Temporal compensation of the photons: (a) spectrum of the two polarizations with the two filter ITU windows; (b) delay induced by the waveguide anisotropy; (c) delays compensated by 6 metres of polarization maintaining fiber.

The measurements were carried out for four fixed analysis bases, the source yielding very good operational parameters as we show in Figure 5.

4. Entanglement with Nuclear Particles

The success of entangled photon quantum key distribution schemes gave way to the perspective of employing other elements as information bearers [17]. Nuclear particles, neutrinos in particular, have little absorption in any media, thus being able to propagate through any environment, at great distances. Other particles, such as muons and leptons, present

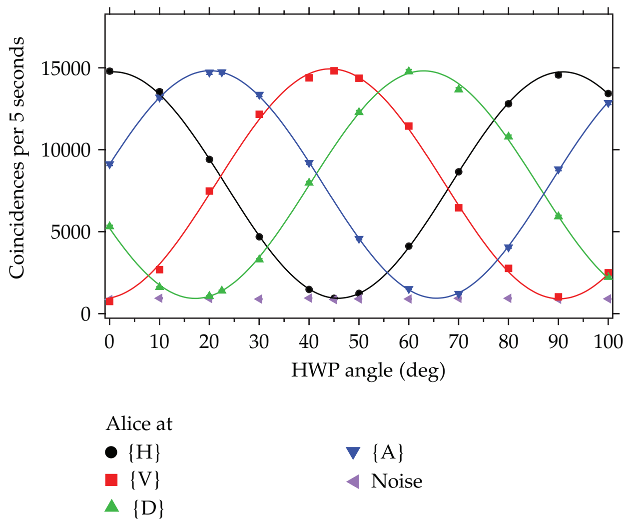

Figure 5: Bell state measurement results.

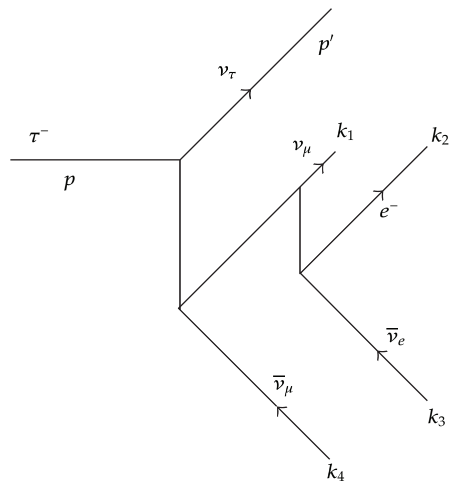

Figure 6: Tau lepton decay process.

almost the same absorption pattern through media. Entangled neutrino states can be generated as a result of the decay interaction:

$$\tau^- \longrightarrow \nu_\tau + \nu_\mu + e^- + \overline{\nu}_\mu + \overline{\nu}_e. \tag{4.1}$$

As shown in Figure 6, the two final antineutrinos symbolized by k_3 and k_4 have almost parallel momenta and thus the same helicity. This makes the total spin wavefunction of the interaction a symmetrical one. The antisymmetric nature of fermions implies that the flavor wavefunction should be antisymmetric. The wavefunction of the two emitted neutrinos will have the form

$$|\psi\rangle = \frac{1}{\sqrt{2}}(\overline{\nu}_e\overline{\nu}_\mu - \overline{\nu}_\mu\overline{\nu}_e) \tag{4.2}$$

for which we have the corresponding Bell inequality

$$S = \frac{P(t_{l_1} = \nu_\mu, \mathcal{A})}{P(\infty, \mathcal{A}) - P(t_{l_2} = \nu_e, \mathcal{A}) + P(t_{l_1} = \nu_\mu, \infty) - P(t_{l_1} = \nu_\mu, t_{r_1} = \nu_e) + P(t_{l_2} = \nu_e, t_{r_1} = \nu_e)} \leq 1, \tag{4.3}$$

where $\mathcal{A}$ denotes $t_{r_2} = \nu_\mu$, t_{l_i}, and t_{r_i} are the evolving times on left and right sides. $P(t, \infty)$ symbolizes the case where all three-flavor triggers on the right side are countered. In this case, the neutrino flavors play the role of polarizations, while the time variation plays the role of angles between them in photon experiments [21, 22, 27].

Further studies showed that there exists a natural quantum key distribution protocol for entangled neutrinos, should the distances of the four detectors from the source be identical. The entangled state makes coincidence counting at Alice and Bob's side be either $\mathrm{AB} = \{\nu_e, \nu_\mu\}$ or $\mathrm{AB} = \{\nu_\mu, \nu_e\}$. If an eavesdropper makes a measurement on Alice and Bob's neutrinos and resends the states, the ensemble state becomes a product state of $|\psi\rangle = |\overline{\nu}_e\overline{\nu}_\mu\rangle$ or $|\psi\rangle = |\overline{\nu}_\mu\overline{\nu}_e\rangle$. In order not to be detected, the eavesdropper must be located at the point where the same flavor countings of A_1B_1 and A_2B_2 are both zero. Thus, as long as the detection distance of the eavesdropper is smaller than the one considered above, it cannot obtain any information without being detected. This is an equivalent property to that of the conventional quantum key distribution protocols such as BB84 or Ek91.

Apart from the tau lepton decay process, neutrinos can be generated from the muon decay process, described by

$$\mu^- \longrightarrow e^- + \overline{\nu}_e + \nu_\mu, \qquad \mu^+ \longrightarrow e^+ + \nu_e + \overline{\nu}_\mu. \tag{4.4}$$

The measured observable in detection modules is the muon ratio, and it is known that the cosmic muon flux and the muon charge ratio are closely linked to the neutrino flux. At lower energies, the trajectories of the muons are influenced by earth's magnetic field. Thus measuring the charge ratio, one obtains quantitative information on the neutrino flux.

From the detection point of view, nuclear particles require a significantly larger and more complex detection apparatus. If, for photons, commercially available Peltier effect cooled InGaAs avalanche photodiodes were sufficient to achieve a good key rate, neutrino detection is carried out inductively, by detecting the flavor of muons and recording the decay times stopped in the detector. Separation of the positive and negative muons, prior to decay observations, is made using magnetic spectrometers. One such detector, containing 20 modules, each of 1 m^2 surface, each composed of an active layer, a 3 cm thick scintillator, wavelength filters, and photocathodes compose the WILLI detection stage [18–20]. This stage has been improved with a rotational module, by removing the lead layers. The mechanical frame of the rotor makes the detector able to move both in azimuth and zenith. Minimizing the dark counts can be achieved by using the modules in anticoincidence.

The extended air shower miniarray (EAS) is part of the detection system and is in charge of measuring the muon charge ratio μ^- / μ^+ produced by the interaction of a primary cosmic ray with the atmosphere. It consists of twelve detection stations placed at about 50 m from the main detector. Each station consists of four scintillator plates, read twofold by a PMT through a wavelength shifter. The electronic scheme behind the detector array is composed of a threshold discriminator, set at −50 mV, providing as output a logical signal which is passed through an FPGA circuit. From the FPGA, each two signals are passed through an OR logical gate and then multiplexed selectively. The resulting signal is then fed to a TDC and QDC acquisition setup. The usual running time of the detector, however, ranges from tenths to hundreds of days, in order to have a statistically correct interpretation of the acquisition data.

5. Conclusions

Summing up all the ideas described in the previous sections, the perspective of successfully extending technologies used in photonic quantum cryptography protocols to nuclear particles becomes an imminent reality with the discovery of usable nuclear entangled states. The nuclear equivalent of spontaneous downconversion can be used to generate flavor-entangled neutrino states, which exhibit extraordinary propagation properties through all media, and thereby overcoming the long-distance-entangled state degradation obstacle. Furthermore, since there is a clear link between neutrinos and other nuclear particles such as muons, one can establish an observable detection link between the two nuclear fluxes. The link consists of a direct proportionality between the muon charge ratio and the neutrino-entangled state, and it can be exploited in a quantitative matter to establish a raw key rate. Experimental data obtained from setups confirm the feasibility of the theoretical issues and expand the application range of quantum key distribution to the nuclear field.

References

[1] A. Einstein, B. Podolsky, and N. Rosen, "Can quantum-mechanical description of physical reality be considered complete?" *Physical Review*, vol. 47, no. 10, pp. 777–780, 1935.

[2] M. Dima, M. Dulea, E. Pauna et al., "The Quantgrid project (Ro)—quantum security in grid computing applications," *Romanian Journal in Physics*, vol. 54, no. 5-6, pp. 441–448, 2009.

[3] O. Danila, M. Demicheli, P. Aschieri, and P. Sterian, "Theoretical studies and simulation of graded index segmented $LiNbO_3$ waveguides for quantum communications," *Optoelectronics and Advanced Materials, Rapid Communications*, vol. 6, pp. 140–243, 2012.

[4] M. Dima, M. Dulea, M. Petre et al., "The QUANTGRID project (RO)—quantum security in GRID computing applications," in *7th International Conference of the Balkan Physical Union*, vol. 1203 of *Proceeding of the AIP*, pp. 461–465, September 2009.

[5] B. A. Stefanescu, D. Anghel, O. Danila, P. Sterian, and A. R. Sterian, "Applications of quantum cryptology for data transmissions implemented in a student laboratory," in *Annals of the Academy of Romanian Scientists*, vol. 5 of *Science and Technology of Information*, no. 1, 2012.

[6] M. Dima, M. Dulea, D. Aranghel et al., "Classical and quantum communications in grid computing," *Optoelectronics and Advanced Materials, Rapid Communications*, vol. 4, no. 11, pp. 1840–1843, 2010.

[7] R. Horodecki, P. Horodecki, and M. H. K. Horodecki, "Quantum entanglement," *Reviews of Modern Physics*, vol. 81, no. 2, pp. 865–942, 2009.

[8] C. Bennett and G. Brassard, "Quantum cryptography: public key distribution and coin tossing," in *Proceedings of the Conference on Computers, Systems and Signal Processing*, pp. 175–179, Bangalore, India, 1984.

[9] A. K. Ekert, “Quantum cryptography based on Bell’s theorem,” *Physical Review Letters*, vol. 67, no. 6, pp. 661–663, 1991.

[10] J. S. Bell, “On the Einstein Podolsky Rosen paradox,” *Physics*, vol. 1195, no. 3, 1964.

[11] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, “Proposed experiment to test local hidden-variable theories,” *Physical Review Letters*, vol. 23, no. 15, pp. 880–884, 1969.

[12] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, “Quantum cryptography,” *Reviews of Modern Physics*, vol. 74, no. 1, pp. 145–195, 2002.

[13] E. Schrödinger, “Die gegenwärtige Situation in der Quantenmechanik,” *Naturewissenschaften*, vol. 23, pp. 807–812, 1935.

[14] D. N. Klyshko, *Photons and Nonlinear Optics*, Gordon and Breach, New York, NY, USA, 1988.

[15] P. E. Sterian and N. N. Puşcaş, *Laseri Si Procese Multifotonice*, Technical Publishing House, Bucharest, Romaina, 1988.

[16] F. Kaiser, A. Issautier, L. A. Ngah et al., “High quality polarization entanglement state preparation and manipulation in standard telecommunications channels,” *New Journal of Physics*, vol. 14, Article ID 085015, 2012.

[17] J. Li and C. F. Qiao, “Quantum entanglement of neutrino pairs,” http://arxiv.org/abs/0708.0291.

[18] B. Vulpescu, J. Wentz, I. M. Brâncuş et al., “A compact detector for the measurement of the cosmic-ray muon charge ratio,” *Nuclear Instruments and Methods in Physics Research Section A*, vol. 414, pp. 205–217, 1998.

[19] B. Vulpescu, J. Wentz, I. M. Brancus et al., “The charge ratio of atmospheric muons below 1.0 GeV c^{-1} by measuring the lifetime of muonic atoms in aluminium,” *Journal of Physics G*, vol. 27, no. 5, pp. 977–991, 2001.

[20] D. Heck, J. Knapp, J. N. Capdevielle, G. Schatz, T. Thouw et al., “CORSIKA: a Monte Carlo code to simulate extensive air showers,” Wissenschaftliche Berichte FZKA 6019, Karlsruhe, Germany, 1998.

[21] B. Mitrica, I. M. Brancusa, H. Rebelb et al., “Experimentally guided Monte Carlo calculations of the atmospheric muon and neutrino flux,” *Nuclear Physics B. Proceedings Supplements*, vol. 151, no. 1, pp. 295–298, 2006.

[22] B. Mitrica, *Studiul dependentei directionale a fluxului de miuoni si posibiltati de testare ale modelelor de interactie hadronica [Ph.D. thesis]*, University of Bucharest, 2010.

[23] C. Iliescu, M. Avram, B. Chen et al., “Residual stress in thin films PECVD depositions: a review,” *Journal of Optoelectronics and Advanced Materials*, vol. 10, no. 4, pp. 387–394, 2011.

[24] C. Iliescu, G. Tresset, F. S. Iliescu, and P. E. Sterian, “Live/Dead cell assay based on dielectrophoresis-on-a-chip,” *UPB Scientific Bulletin, Series A*, vol. 72, no. 1, pp. 33–44, 2010.

[25] F. S. Iliescu, A. P. Sterian, E. Barbarini, M. Avram, and C. Iliescu, “Continuous separation of white blood cell from blood in a microfluidic device,” *UPB Scientific Bulletin, Series A*, vol. 71, no. 4, pp. 21–30, 2009.

[26] C. Iliescu, H. Taylor, M. Avram, J. Miao, and S. Franssila, “A practical guide for the fabrication of microfluidic devices using glass and silicon,” *Biomicrofluidics*, vol. 6, no. 1, Article ID 016505, 2012.

[27] H. Rebel, O. Sima, A. Haungs, C. Manailescu, B. Mitrica, and C. Morariu, “The muon charge ratio in cosmic ray air showers,” *Journal of Physics G*, vol. 35, no. 8, Article ID 085203, 2008.

Journal of
Gravity
Journal of
Photonics
The Scientific
World Journal
Journal of
Soft Matter
Advances in
Condensed Matter Physics
Journal of
Fluids
Journal of
Aerodynamics
Hindawi
Submit your manuscripts at
http://www.hindawi.com
International Journal of
Statistical Mechanics
International Journal of
Optics
Journal of
Computational
Methods in Physics
Advances in
High Energy Physics
Journal of
Thermodynamics
Physics
Research International
Advances in
Astronomy
Journal of
Solid State Physics
Journal of
Astrophysics
International Journal of
Superconductivity
Journal of
Biophysics
Journal of
Atomic and
Molecular Physics