World Academy of Science, Engineering and Technology
International Journal of Nuclear and Quantum Engineering
Vol:5, No:7, 2011

Compton Scattering of Annihilation Photons as a Short Range Quantum Key Distribution Mechanism

Roman Novak and Matjaž Vencelj

***Abstract*—**The angular distribution of Compton scattering of two quanta originating in the annihilation of a positron with an electron is investigated as a quantum key distribution (QKD) mechanism in the gamma spectral range. The geometry of coincident Compton scattering is observed on the two sides as a way to obtain partially correlated readings on the quantum channel. We derive the noise probability density function of a conceptually equivalent prepare and measure quantum channel in order to evaluate the limits of the concept in terms of the device secrecy capacity and estimate it at roughly 1.9 bits per 1 000 annihilation events. The high error rate is well above the tolerable error rates of the common reconciliation protocols; therefore, the proposed key agreement protocol by public discussion requires key reconciliation using classical error-correcting codes. We constructed a prototype device based on the readily available monolithic detectors in the least complex setup.

***Keywords*—**Compton scattering, gamma-ray polarization, quantum cryptography, quantum key distribution

I. Introduction

ALTHOUGH rarely recognized as being practical, quantum key distribution (QKD) over a short distance has its applications that range from building access control to secure identification of devices, components and systems. The usual argument of having much easier ways of generating a common secret key if not separated by macroscopic distance does not apply to high security environments that involve mobile communicating parties and where security tokens based on the unconditional or information-theoretic security have priority over those relying on the intractability of well-known mathematical problems. For example, certain military grade applications would require establishing session keys strong enough to withstand any cryptanalysis even if the two parties have the ability to actually make a physical contact. Ideally, a one-time pad would be employed based on a shared secret key that could be arbitrarily extended. In those applications, the fact that key distribution is a short range one by laws of nature offers an additional protection as it further limits the location of an adversary.

The majority of QKD efforts relate to visible or infrared light, since it can travel distances without decoherence. In contrast to our approach, which is inherently short range, long range QKD over fibre is typically targeted in the current research [1]. Free-space QKD is also gaining momentum [2], [3], including its applications to satellite communications [4]. Here we study the use of gamma photons as short range information carriers, the detection of which is also well-understood and extensively done in practice. Our approach is entanglement-based (EB), as it is not easy to prepare gamma quanta in a particular state.

The basic elements of QKD are well known [5]. At this point we only give a short overview of an EB setting which suffices for the rest of the paper. Two legitimate parties, usually denoted as Alice and Bob, are connected by a quantum as well as by a classical communication channel. Alice owns a positron emission source, placed at the center of the setup and allowing annihilation photons to be detected by both parties. The geometry of Compton scattering is measured on both sides as a way to obtain partially correlated readings on the quantum channel. Usual assumptions about the QKD apply. Alice and Bob initially share an authentication key which enables detection of modified or fraudulent messages on the public channel, effectively limiting an eavesdropper Eve to a read-only access to the public channel.

On the quantum channel, the uncertainty principle prevents an eavesdropper from obtaining the exact same reading as the legitimate parties and, at the same time, imposes bounds on the expected error rate for both, an uncompromised and a compromised quantum channel.

II. Physical Layer

The type of interaction of a gamma photon with matter depends on its energy and the material that is in the way. Compton scattering is dominant in most materials at the energies specific for the annihilation photons. In aluminum, for instance, the photoelectric absorption of 511 keV quanta is some 600 times less probable than Compton scattering, whereas photonuclear reactions and pair production are practically negligible. The polarization is a quantum degree of freedom that we propose here to convey the information on a quantum channel, the same variable that was used in the numerous quantum key distribution proposals using light quanta, starting with the BB84 [6]. If a positron annihilates with an electron in a system having effectively a zero angular momentum, two photons are emitted in the opposite directions having polarizations of their electric fields perpendicular to each other. The polarization of each photon presents itself to a measuring party through the azimuthal scattering angle of the subsequent Compton interaction. In the schematic depiction of a single Compton interaction in Fig. 1, the scattering plane is defined by the incident and the scattered photon directions k_0 and k_1, whereas the azimuthal angle η is the angle between

R. Novak is with the Department of Communication Systems, Jožef Stefan Institute, Ljubljana SI-1000, Slovenia (phone: +386-1477-3109; fax: +386-1477-3111; e-mail: roman.novak@ijs.si).

M. Vencelj is with the Department of Low and Medium Energy Physics, Jožef Stefan Institute, Ljubljana SI-1000, Slovenia (e-mail: matjaz.vencelj@ijs.si).

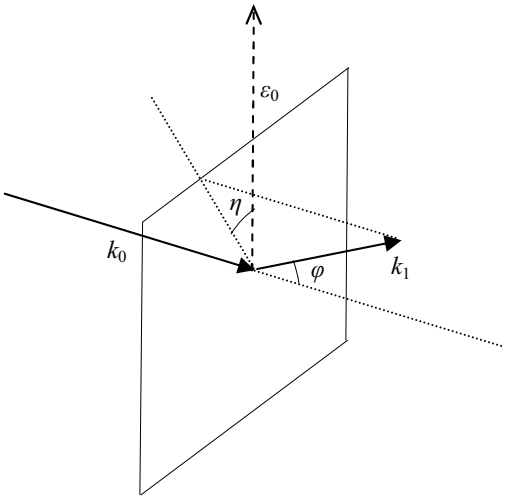

Fig. 1. Compton interaction with a free electron; primary quantum k_0 scatters in direction of k_1 at an angle φ with respect to the incident direction, and at an azimuthal angle η relative to the electrical vector ε_0.

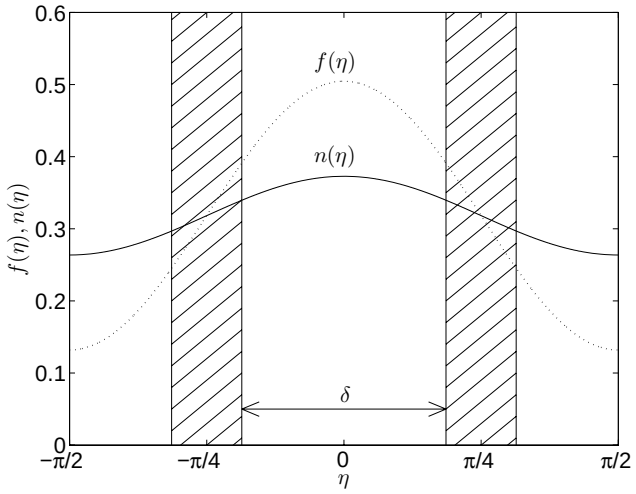

Fig. 2. Periodic extension of the noise pdf due to Compton scattering of linearly polarized photons; scattering angles are limited to $50° \leq \varphi \leq 110°$. The conceptual P&M noise (solid line) is plotted alongside the ideal measurement noise at Alice's and Bob's side (dotted line). The shaded areas indicate η-ignored events in the binary protocol.

the scattering plane and the electrical vector ε_0 of the incident photon.

The scattering cross section of a plane-polarized incident radiation is described by the well-known Klein-Nishina formula [7], which can be expressed as

$$\frac{d\sigma}{d\Omega} = \frac{r_0^2}{2}\left(\frac{h\nu'}{h\nu}\right)^2\left(\frac{h\nu'}{h\nu} + \frac{h\nu}{h\nu'} - 2\sin^2\varphi\cos^2\eta\right), \quad (1)$$

where $d\sigma$ is the differential scattering cross section, $d\Omega = \sin\varphi\, d\varphi\, d\eta$ is the differential solid angle for the scattered photon, r_0 is the classical electron radius, $h\nu$ and $h\nu'$ the energies of the incoming and the outgoing photon, φ is the scattering angle, and η is the azimuthal angle introduced earlier.

The EB quantum channel can conceptually be modeled as the more common prepare and measure quantum channel (P&M), the latter being equivalent to a noisy communication channel for which the equivalent noise probability density function (pdf) follows from (1). The measurements of η on both sides of the channel are correlated [8] with a systematic offset of $\pi/2$ and take on values from 0 to 2π, which can obviously be mapped on $[0, \pi)$ with η and $\eta + \pi$ representing the same polarization direction. The equivalent noise is not limited in amplitude whereas the azimuthal measurement is done modulo π and thus always maps into a finite interval, meaning that (1) actually determines the periodic extension of noise pdf independently at each channel side. Suppose that scattering angles considered are bounded by $\varphi_{\mathrm{L}} \leq \varphi \leq \varphi_{\mathrm{H}}$ due to the reasons stated later, then the cross section for a linearly polarized photon to be scattered into different azimuthal angles is given by

$$d\sigma_{\mathrm{LH}}(\eta) = d\eta \int_{\varphi_{\mathrm{L}}}^{\varphi_{\mathrm{H}}} \frac{d\sigma}{d\Omega}\sin\varphi\, d\varphi, \quad (2)$$

where the kinematic relationship between $h\nu'$ and $h\nu$ for the scattered photons with an initial energy of $m_{\mathrm{e}}c^2$ equals

$$\frac{h\nu'}{h\nu} = \frac{1}{2 - \cos\varphi}. \quad (3)$$

The azimuthal cross section has a maximum at $\pi/2$, which sets the origin of the periodic noise pdf

$$f(\eta) = \frac{d\sigma_{\mathrm{LH}}(\eta - \frac{\pi}{2})}{d\eta} \Big/ \int_0^{\pi} \frac{d\sigma_{\mathrm{LH}}(\eta)}{d\eta}\, d\eta. \quad (4)$$

Having two independent periodic extensions of noise pdf on Alice's and Bob's side, the periodic extension of the equivalent prepare and measure noise is a circular convolution

$$n(\eta) = \int_0^{\pi} f(\tau) f(\eta - \tau)\, d\tau. \quad (5)$$

Sample $f(\eta)$ and $n(\eta)$ for arbitrarily chosen φ_{L} and φ_{H} are plotted in Fig. 2.

III. Key Distribution Protocol

The following baseline key agreement protocol by public discussion can be applied without loss of generality. Let S denote a random variable reflecting the actual polarization of the incident photon as generated by the source in Alice's direction, given as an azimuthal angle relative to some transversal base vector. Alice and Bob have random variables X and Y at their disposal, respectively, by measuring S via Compton scattering. Alice computes $X+V$, where V is the key data, and sends the result over the public channel to Bob, who approximates V by the difference $X+V-Y-\pi/2$. In terms of the equivalent P&M quantum channel Alice chooses both random variables X and V, sends X over the quantum channel and $X+V$ over the public channel, whereas Bob's computation results in $V+E$, with E being the equivalent P&M noise distributed

according to (5) and, in a real scenario, including additional measurement noise from both sides.

The information about V available to the eavesdropper on the public channel must effectively be kept at a minimum, i.e., the mutual information $I(V;X+V)$ must be close to zero. Because X and V are independent, meaning that $I(V;X+V)=H(X+V)-H(X)$, zero mutual information is achieved for the maximum entropy $H(X)$, implying a uniform distribution of X. Note that the uniform distribution is the maximum entropy distribution among the continuous distributions supported on a given interval and that $X+V$ is supported on the same interval as X. Although S is being generated by an isotropic annihilation source owned by Alice, the distribution of X, being the measurement of S, does not necessarily comply with the requirement. Therefore, the measurement subsystem must correct for possible deviations as much as possible. Some leaked information could successfully be reduced to an arbitrarily small amount by a higher layer privacy amplification protocol [9], [10].

IV. Bounds on the Secret Key Rate

Given the quantum channel based on the polarization correlation of entangled gamma-ray quanta as measured through Compton scattering, the important question arises on the limits of the concept in terms of the maximal secret key rate, known also as the channel secrecy capacity. Informally, the secrecy capacity is the maximum number of bits per channel use that Alice can send to Bob in secrecy with an arbitrarily small error probability. In addition to the channel secrecy capacity, which refers to the considered coincident events, the device secrecy capacity is of significant importance as it measures the maximal secret key rate per emitted photon pair.

Here we build on the results of Maurer [11], who derived bounds on the secret key rate for the closely related problem of the secret key agreement by public discussion when two parties possess correlated random variables X and Y recovered from a noisy broadcast channel. An eavesdropper generally obtains some information as random variable Z. An example of such a scenario is a satellite broadcasting random bits while the involved parties exploit partial independence of the received noise to agree on a secret key. As opposed to the broadcast channel, the leakage of information to Eve on our quantum channel could be detected and ruled out at a given confidence level based only on the error rate measurement as discussed later. The most general result, having $I(X;Z)$ and $I(Y;Z)$ both equal to zero, is that the secret key rate of X and Y is tightly bounded by $I(X;Y)$.

Achieving a key agreement rate matching the mutual information $I(X;Y)$ requires the use of theoretically optimal error-correcting schemes in which the uncertainty of the measurement must assist the encoding/decoding process. In addition to η, precise measurements of φ on both sides would also be a prerequisite. While the solution is appealing, it turns out to be computationally demanding and impractical for our proof-of-concept study. Here we investigate a simpler scenario where limited or no information about the scattering angle is required, which, among other simplifications, allows building a prototype device based on the readily available monolithic detectors and still provides a good estimate on the secrecy capacity bounds.

Let us define a binary encoder/decoder consisting of encoding, $V=e(K)$, and decoding, $K'=d(V+E)$, transformations, where e and d are defined as

$$e(x)=\begin{cases}0, & x=0\\ \frac{\pi}{2}, & x=1\end{cases} \tag{6}$$

and

$$d(x)=\begin{cases}0, & -\frac{\pi}{4}\le x<\frac{\pi}{4}\\ 1, & \text{else}\end{cases}. \tag{7}$$

Basically, a binary key $K\in\{0,1\}$ is mapped into two orthogonal angles and later approximated by the most probable value. Using e and d, we obtain an equivalence with the binary symmetric broadcast channel. Let h denote the binary entropy and ϵ the bit error probability, i.e., $P(k'\mid k)=1-\epsilon$ if $k=k'$, and $P(k'\mid k)=\epsilon$ if $k\neq k'$. The channel secrecy capacity is then given by $1-h(\epsilon)$.

Before looking at the bit error probability ϵ for pairwise Compton events, we first establish some additional terms, which are needed for deriving an upper bound on the device secrecy capacity. Scatter efficiency k_{S} gives the proportion of the emitted entangled photons scattered by Alice and Bob in coincidence. Clearly, k_{S} depends on the device design choices.

Ideally, all the coincident events should be used as the information passing carriers in order to maximize the secret key rate if a near-optimal error-correcting scheme is in place. On the other hand, applying the binary encoder/decoder, some events are better ignored for higher key rate because their uncertainty decreases the final rate more than if they were left out completely. Let k_φ be the proportion of coincidences with a favorable scattering angle $\varphi_{\mathrm{L}}\le\varphi\le\varphi_{\mathrm{H}}$ simultaneously on both sides,

$$k_\varphi=\left(\frac{1}{\sigma}\int_0^{2\pi}\frac{d\sigma_{\mathrm{LH}}(\eta)}{d\eta}\,d\eta\right)^2. \tag{8}$$

The formula takes into account the independence of the pairwise scattering angles and the total cross section σ for 511 keV photons.

The same reasoning applies to the difference in the azimuthal angles. The uncertainty of the decoder is the largest at $x=\pm\pi/4$, which is why restricting the actually considered differences to those closer to 0 and $\pi/2$ results in a higher key rate. k_η gives the proportion of considered events among k_φ events based on the η-difference,

$$k_\eta=\int_{-\frac{\delta}{2}}^{\frac{\delta}{2}}n(\eta)\,d\eta+\int_{\frac{\pi}{2}-\frac{\delta}{2}}^{\frac{\pi}{2}+\frac{\delta}{2}}n(\eta)\,d\eta, \tag{9}$$

where δ sets the limits for acceptable events as depicted in Fig. 2. Bit error rate per considered event is thus calculated as

$$\epsilon=\frac{1}{k_\eta}\int_{\frac{\pi}{2}-\frac{\delta}{2}}^{\frac{\pi}{2}+\frac{\delta}{2}}n(\eta)\,d\eta, \tag{10}$$

TABLE I
OPTIMAL BINARY ENCODER/DECODER PARAMETERS

φ_{L}	φ_{H}	δ	k_φ	k_η	k_{S}	ϵ	$S(X,Y)$
40°	129°	67°	0.343	0.745	1	0.449	0.0019

leading to the maximum device secret key rate being the solution of the following optimization problem

$$S(X,Y) = k_{\mathrm{S}} \max_{\varphi_{\mathrm{L}},\varphi_{\mathrm{H}},\delta} \left(k_\varphi k_\eta \left(1 - h(\epsilon)\right)\right). \tag{11}$$

A quantitative solution to (11) using numerical integration and a 1-degree resolution for φ_{L}, φ_{H} and δ is given in Table I.

The quoted bit error rate is close to the limit value of 0.5, at which any key agreement would be impossible, and draws severe constraints on the higher layer protocols. Information reconciliation should take place first in order to correct the errors and perfectly correlate Alice's and Bob's keys, followed by the privacy amplification step. Interactive reconciliation protocols, such as the protocols with several rounds of parity check [12], [13] or more recent method based on combinatorial group testing [14] have tolerable bit error rate well below our estimate, leaving classical error-correcting code approach as the most viable choice, at least to align the key bits to a degree that would render other approaches effective. Although extremely inefficient in a low bit error regime, repetition codes may prove to be a good choice here. Further investigation of the soft-decoding error correcting schemes is needed that would benefit from the well-defined noise. At this point of analysis, Table I suggests that no more than 2 shared bits can be agreed in secrecy from 1000 annihilation events. Assuming k_{S} close to 1, which is not too unreasonable as discussed later under the architectural considerations, a key data rate of 500 bits/s can be expected using a moderately active β^+ source of 300 kBq (a license exempt activity of ^{22}Na under the EU and US jurisdictions) and 80% theoretically efficient error-correcting code.

V. INTRUDER DETECTION

Since an intruder is subject to the same physical laws as the legitimate communicating parties, a degradation of the quantum channel is unavoidable on any attempt of eavesdropping. Related quantum principles prohibit multiple measurements of a single particle in its original state, whereas an intercept and resend technique fails to replicate more than one bit of the polarization information due to the uncertainty principle. Note that photon number splitting attack [15] pose no threat because of the use of a single photon source. Therefore, public comparison of some bits, which are discarded later as key material, necessarily leads to the detection of an intruder, upon which Alice and Bob can postpone or cancel entirely the key agreement procedure.

Let us assume that Eve has the ability to measure the polarization with the smallest theoretically possible uncertainty and produce a photon with the exact measured polarization, although, to the best of our knowledge, no current technology supports this at the energies of interest. The bit error rate ϵ' would be observed by Alice and Bob, for which the lower bound can be computed by convolving an ideal cosine noise

$$e(\eta) = \frac{2}{\pi}\cos^2\eta \tag{12}$$

with (5) and substituting $n(\eta)$ with the result. Equation (10) now gives ϵ', which evaluates at 0.479 for the parameters in Table I. Note that ϵ can be larger from the calculated one, in which case ϵ' also increases.

Standard hypothesis testing techniques can be applied as a part of the intruder detection procedure. In order to identify an eavesdropper on the quantum channel with a given confidence level $1-\alpha$ we can adopt a null hypothesis that the error rate is greater or equal to ϵ'. The number of measured erroneous bits, assuming the null hypothesis is true, follows the binomial distribution $B(N,\epsilon')$, which can be approximated by the normal distribution $N(N\epsilon', N\epsilon'(1-\epsilon'))$ when the number of inspected bits N is large enough. Further, the probability β of a failure to reject the null hypothesis when there is no intruder can be calculated since in this case the distribution actually follows $B(N,\epsilon)$. For example, to reduce the probability of incorrectly rejecting the null hypothesis to less than 1 in a million, i.e., not detecting an eavesdropper at $\alpha = 10^{-6}$, the threshold number of erroneous bits should be set at 9 244 out of 20 000 randomly selected bits. At the same time, the probability of falsely rejecting the communication remains low at $\beta = 8.6 \times 10^{-5}$, taking the bit error rates as calculated previously.

VI. ARCHITECTURAL CONSIDERATIONS

Employing two position-sensitive segmented detectors, as illustrated in Fig. 3, allows for measurements of the scattering geometry. The architecture could support an implementation of the proposed binary encoder/decoder protocol as well as more complex protocols. The detectors, belonging to Alice and Bob, are placed alongside each other with the annihilation source in between. They are big enough to capture the majority of the emitted photon pairs irrespective of their incident directions, i.e., having k_{S} approach 1. Each detector serves as a scatterer and detects the interaction positions and deposited energies of the incident and of the scattered photons, which may provide an additional help in cancelling out the background. Further, in any real application, the scattered photons that cross the detectors middle boundary should preferably be vetoed out because any further correspondence between Alice and Bob than that allowed by the protocol must be avoided in order not to introduce security vulnerabilities.

An actual realization of the 3D setup would naturally be penalized by the factors such as finite detector size, finite spatial and energy resolution, coincidence resolving time resolution and scattering to photoabsorption ratios of the detector material. Although a conceptually simple architecture, it is still technically challenging to build. For instance, a state-of-the-art room-temperature spatially sensitive CdZnTe detector could resolve the lateral position of the interaction point by anode pixellization, whereas the interaction depth measurement requires a precise analysis of the electron drift time, resulting

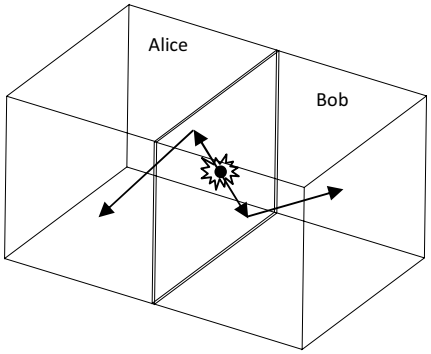

Fig. 3. Device setup based on the spatially sensitive detectors; the architecture can support the binary encoder/decoder protocol, while also allowing for more complex error correcting codes and a technically challenging multiple scatter quantum cryptography.

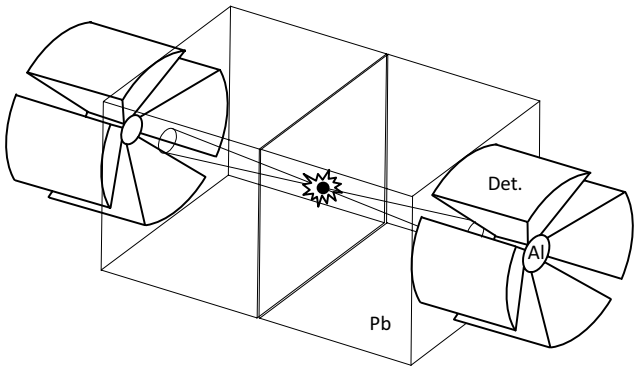

Fig. 4. A technically less challenging setup based on several monolithic detectors. The cone shaped channel in the shield collimates photons in the direction of the scatterer, which is surrounded by the four detectors.

in an increased complexity of the signal processing electronics [16].

The fact that the majority of scatter events are available for processing and that the angles are actually measured, make this architecture ideal for the near-optimal error correcting codes that would benefit from the information on the uncertainty of the measured polarization. Furthermore, for a polarized incident photon the scattered photon is also completely polarized with the angle between the directions of polarization described by the Klein-Nishina formula. The scattered photon with the reduced energy may get involved in further Compton interactions, which could reveal additional information on the original polarization. Note, however, that the probability of a photoelectric interaction increases at lower energies. The sole detection of multiple events and the complexity of mathematical treatment of such multi-level scattering rise significant applicability concerns.

By a slight adaptation of the baseline key distribution protocol, the device complexity reduces significantly at the expense of a higher error rate. Suppose Alice's and Bob's ability to measure azimuthal angles is restricted to two polarization states, for instance vertical and horizontal, with an intermediate polarization being mapped to the closest match. Variables X and Y given earlier should now be treated as symmetric random binary variables. Although we cannot treat the η-difference as before, a similar albeit less pronounced tradeoff can be exploited on each side by ignoring tight polarization decisions. As a consequence, k_η should be redefined as

$$k_\eta = \frac{1}{\pi}\int_0^{\pi}\Big[\int_{-\frac{\delta}{2}}^{\frac{\delta}{2}} f(\eta-\tau)\,d\eta + \int_{\frac{\pi}{2}-\frac{\delta}{2}}^{\frac{\pi}{2}+\frac{\delta}{2}} f(\eta-\tau)\,d\eta\Big]^2\,d\tau. \quad (13)$$

The proportion of considered events is now calculated from the original periodic noise pdf at each side, while taking the average over uniformly distributed photon polarizations. The bit error rate should be rewritten as follows:

$$\epsilon = \frac{2}{\pi k_\eta}\int_0^{\pi}\Big[\int_{-\frac{\delta}{2}}^{\frac{\delta}{2}} f(\eta-\tau)\,d\eta \int_{\frac{\pi}{2}-\frac{\delta}{2}}^{\frac{\pi}{2}+\frac{\delta}{2}} f(\eta-\tau)\,d\eta\Big]\,d\tau. \quad (14)$$

Solving (11) using (13) and (14) gives the same optimal angles and k_φ as shown in Table I. The error rate ϵ increases to 0.460 at $k_\eta = 0.556$, resulting in 0.0009 secret key bits per scatter coincidence. The threshold error rate ϵ' for detecting Eve increases to 0.480.

A device architecture that could be considered as an approximation to the simplified model is shown in Fig. 4. Alice's and Bob's devices are delimited by the radiation source in the center. The gamma-ray field is first collimated by a cone shaped channel in the lead block of each device. The photons are then scattered by the aluminum scatterers in the shape of a truncated cone and detected by one of the four detectors. The equidistant spacing and the shape of each detector approximate optimal geometry for a single point of scatter in an attempt to maximize the secret key rate for a device using only monolithic detectors.

VII. Experimental Setup

The concept underlying the proposed QKD device has already been confirmed experimentally in 1948 [17]. Charting the key experimental considerations relevant to any practical implementation of the proposed quantum channel requires event-by-event analysis using current detector technology. Therefore, we constructed a full working prototype of the QKD device based on two gamma polarimeters in the least complex setup we could conceive for the task based on the architecture of Fig. 4.

The annihilation radiation source used was 250 kBq of ^{22}Na, decays of which lead in nearly 90% [18] to the emission of three coincident gamma rays: a pair of 511 keV annihilation photons with nearly collinear trajectories and a 1.275 MeV relaxation of the daughter nucleus ^{22}Ne.

The source was sandwiched between two cylindrical lead shields, bored through for collimation of two diametrically opposite beams of gamma rays. Each of the beams got intercepted by a cylindrical aluminum scatterer. Two scintillation detectors were placed to the sides of each scatterer, as shown in Fig. 5.

Dimensionally, the experimental geometry was designed reversely from the four identical $1/2" \times 1/2"$ NaI(Tl) scin-

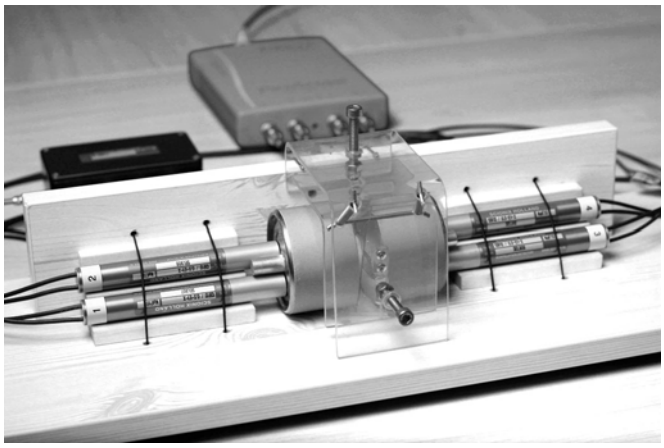

Fig. 5. Prototype QKD device consisting of an annihilation radiation ^{22}Na source, two cylindrical lead shields with the collimation channels, two cylindrical aluminum scatterers and four detectors with the data acquisition electronics.

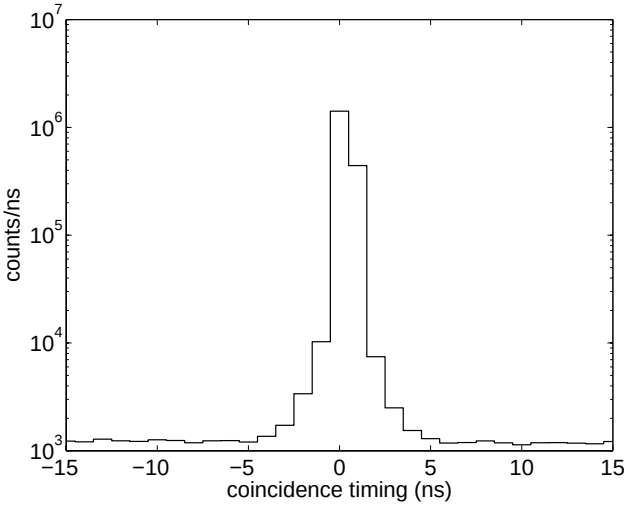

Fig. 6. Spectrum of the measured time difference between pulses in detectors at positions 1 (bottom-left) and 4 (top-right). Note the log scale on the vertical axis—there were nearly no chance coincidences.

tillation detectors by Scionix that we have available in the laboratory.

The scatter cylinders were made of aluminum for its high ratio of Compton scattering to photoelectric absorption of 511 keV photons. The cylinder diameter was chosen at 1 cm to limit the absorption of already scattered outgoing 250 keV photons. At the same time, a tight proximity of the detectors to the scatterers is dictated if one is not to lose a prohibitive proportion of detector solid angle coverage. A cylinder length of 2 cm was a compromise between primary beam penetration into aluminum and the targeted range of detectable scattering angles at given detection crystal shape.

Two cylindrical lead shields were cast, each 4 cm thick and 6.5 cm in diameter, with a graduated 8 mm to 10 mm diameter collimation channel. The thickness was chosen such that the signal of interest for QKD would dominate over direct shield penetration by the 1275 keV gamma rays, while maintaining as much solid angle coverage by the aluminum scatterers as possible.

Raw anode signals from the four photomultipliers were terminated with 50 Ω at the inputs of a PicoScope 4424 digitizer, set at 20 MS/s on each channel. Following a hardware trigger, software was set to store coincident events only (i.e., events where any two of the four detectors fired at the same instant, to within a few nanoseconds) to mass storage media as digitized scope trace snippets. Detectors were also swapped between positions to rule out systematic deviations of single detection channels from biasing the end result.

VIII. Experimental Results

Given the weak source of positrons and a rather inefficient detection geometry, it took some 180 hours of data acquisition to collect 1 892 452 coincident events. Fig. 6 shows an extremely clean coincidence timing spectrum revealing that there were nearly no chance coincidences. The coincident timing window was then reduced to ±1 ns.

A vast 1 813 923 of collected events were single-side coincidences where two detectors fired on the same side of the quantum channel. Most of these events were due to a 1275 keV photon penetrating the lead collimator, then scattering off one detector into the other one on the same side. There were further 1259 triple coincidences along with 33 quadruples when one or both detectors on the other side fired as well. None of these events support polarization-encoded information transport over the channel.

Of the remaining 77 171 events, 40 627 were coincidences of either detection positions 1 and 4, or 2 and 3 (bottom-left and top-right, or top-left and bottom-right in Fig. 5), corresponding to the expected correlation of perpendicular quanta polarization. 36 544 events were of the other symmetry.

Since the channel capacity is so sensitive to the channel error rate, it pays to impose an additional energy range constraint on the dataset, reducing the error rate at the expense of experimental statistics. A maximal secret key rate (proportional to the product of the number of valid events and channel capacity $1 - h(\epsilon)$) is reached when only events depositing between 25 keV and 470 keV in each detector were considered.

The upper energy limit of 470 keV is consistent with a gamma ray scattering within the first few millimeters of the aluminum cylinder at a shallow angle into the far side of the NaI crystal. The lower limit of 25 keV however is so low due to the fact that gamma rays of a few hundred keV show in NaI comparable cross sections for Compton scattering and for photoelectric absorption. Given the small crystal size of one half inch, a single interaction is the most probable case and gamma rays are thus very likely to deposit less than their full energy in the detector. These events turned out to be worth keeping despite the strong background of the lead X-ray peak at roughly 80 keV.

Fig. 7 shows how the detected energy spectra for each correlation symmetry look after having imposed the energy constraints. This illustrates the final experimental statistics that consists of 30 840 events in favorable scattering geometry

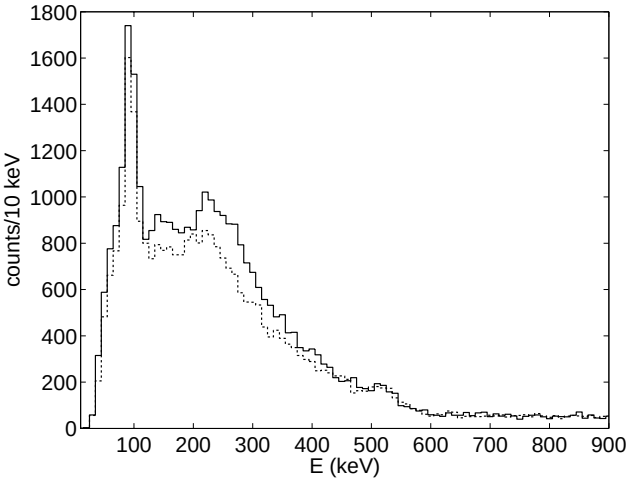

Fig. 7. The energy spectra of a fully filtered dataset, shown for one channel whith the energy constraint imposed for the coincident counterpart event. The solid line spectrum bins the favorable (information carrying) events, whereas the dashed line illustrates the events of the other scattering symmetry.

and 26 418 events contributing to the erroneous key bits. The bit error rate of the experimental quantum channel is thus 0.461(2), defining via the binary entropy a channel capacity of 0.0043(5) to yield a maximum information transfer of 247(30) error-free quantum key bits within the collected statistics for this specific experimental geometry.

IX. Conclusion

We have demonstrated the applicability of the Compton scattering of entangled gamma-ray quanta to the QKD problem. We believe that a carefully designed device has a potential to provide an adequate secret key rate to fulfill some real-life requirements. Furthermore, such a device is technically less complex than today's commercially available QKD products. Our specific implementation of the QKD differs from all others known to date in that it supports QKD across thin walls, e.g., plasterboard, acrylic, or some millimeters of metallic sheeting. This can be of key importance with RF-tight shelters, data vaults or air-tight chemical/microbial barriers. The main drawback of the approach is the presence of radioactive material in the device, whereas the short range nature could actually be an advantage in some applications.

Acknowledgment

We gratefully acknowledge Mr. Janez Burger and the Institute of Oncology Ljubljana that have kindly let us use their quadruple of NaI(Tl) detectors for this experiment.

References

[1] R. J. Collins *et al.*, "Quantum key distribution system in standard telecommunications fiber using a short wavelength single photon source," *J. Appl. Phys.*, vol. 107, no. 7, pp. 073 102–6, April 2010.
[2] T. Schmitt-Manderbach *et al.*, "Experimental demonstration of free-space decoy-state quantum key distribution over 144 km," *Phys. Rev. Lett.*, vol. 98, no. 1, pp. 01 504–4, January 2007.
[3] A. Restelli *et al.*, "Improved timing resolution single-photon detectors in daytime free-space quantum key distribution with 1.25 GHz transmission rate," *IEEE J. Sel. Topics Quantum Electron.*, vol. 16, no. 5, pp. 1084–1090, September/October 2010.
[4] A. Tomaello, C. Bonato, V. D. Deppo, G. Naletto, and P. Villoresi, "Link budget and background noise for satellite quantum key distribution," *Advances in Space Research*, vol. 47, no. 5, pp. 802–810, March 2011.
[5] V. Scarani, H. Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution," *Rev. Mod. Phys.*, vol. 81, no. 3, pp. 1301–1350, July/September 2009.
[6] C. H. Bennet and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proc. IEEE Int. Conf. on Computers, Systems and Signal Processing*, Bangalore, India, 1984, pp. 175–179.
[7] O. Klein and Y. Nishina, "Über die streung von strahlung durch freie elektronen nach der neuen relativistischen quantendynamik von dirac," *Zs. f. Phys.*, vol. 52, pp. 853–864, 1929.
[8] H. S. Snyder, S. Pasternack, and J. Hornbostel, "Angular correlation of scattered annihilation radiation," *Phys. Rev.*, vol. 73, no. 5, pp. 440–448, March 1948.
[9] C. H. Bennet, G. Brassard, and J. M. Robert, "Privacy amplification by public discussion," *SIAM J. Computing*, vol. 17, no. 2, pp. 210–229, 1988.
[10] Y. Watanabe, "Privacy amplification for quantum key distribution," *J. Phys. A: Math. Theor.*, vol. 40, no. 3, pp. F99–F104, January 2007.
[11] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inf. Theory*, vol. 39, no. 3, pp. 733–742, May 1993.
[12] G. Brassard and L. Salvail, "Secret-key reconciliation by public discussion," in *Proc. EUROCRYPT'93*, ser. Lecture Notes in Computer Science, vol. 765, 1993, pp. 411–423.
[13] T. Sugimoto and K. Yamazaki, "A study on secret key reconciliation protocol Cascade," *IEICE Trans. Fundamentals*, vol. E83-A, no. 10, pp. 1987–1991, 2000.
[14] J. Fang, Z. L. Jiang, S. M. Yiu, and L. C. K. Hui, "Checking key integrity efficiently for high-speed quantum key distribution using combinatorial group testing," *Optics Communications*, vol. 284, no. 1, pp. 531–535, January 2011.
[15] S. Félix, N. Gisin, A. Stefanov, and H. Zbinden, "Faint laser quantum key distribution: eavesdropping exploiting multiphoton pulses," *J. Mod. Opt.*, vol. 48, no. 13, pp. 2009–2021, 2001.
[16] D. Xu, Z. He, and F. Zhang, "Detection of gamma ray polarization using a 3-D position-sensitive CdZnTe detector," *IEEE Trans. Nucl. Sci.*, vol. 52, no. 4, pp. 1160–1164, August 2005.
[17] E. Bleuler and H. L. Bradt, "Correlation between the states of polarization of the two quanta of annihilation radiation," *Phys. Rev.*, vol. 73, no. 11, p. 1398, June 1948.
[18] R. Sherr and R. H. Miller, "Electron capture in the decay of Na^{22}," *Phys. Rev.*, vol. 93, no. 5, pp. 1076–1081, March 1954.