Laser Physics Letters

Astro Ltd.

LETTER

Active basis choice for quantum key distribution with entangled states

To cite this article: P M Vinetskaya *et al* 2023 *Laser Phys. Lett.* **20** 055201

IOP Publishing | Astro Ltd Laser Physics Letters

Laser Phys. Lett. **20** (2023) 055201 (7pp) https://doi.org/10.1088/1612-202X/acc246

Letter

Active basis choice for quantum key distribution with entangled states

P M Vinetskaya[1,2], **K S Kravtsov**[1,2,*], **N A Borshchevskaia**[1], **A N Klimov**[1] **and S P Kulik**[1]

[1] MSU Quantum Technology Centre, Moscow, Russia
[2] National Research University Higher School of Economics, Moscow, Russia

E-mail: ks.kravtsov@gmail.com

Received 5 March 2023
Accepted for publication 6 March 2023
Published 20 March 2023

Abstract

Entangled quantum key distribution (QKD) is a promising way to generate pairs of unconditionally secret keys. In this paper we review possible realizations of entanglement-based QKD and assess their feasibility in terms of implementation complexity and provided security. We also propose a novel active basis choice approach that enables to use only one single-photon detector per user. The paper provides all necessary details including the required electro-optic crystal configurations to implement such a scheme experimentally.

Keywords: quantum key distribution, quantum cryptography, entanglement

(Some figures may appear in colour only in the online journal)

1. Introduction

Quantum key distribution (QKD) is a mature and at the same time challenging field that brings together quantum physics, cryptography, and photonics. Despite of more than two decades-long history, the problem of building secure and yet simple QKD systems with a clear theoretical foundation is still far from been comprehensively solved.

The most commonly implemented QKD systems are based on prepare-and-measure protocols, i.e. they assume interaction between a transmitter (Alice) and a receiver (Bob) of quantum states. An alternative approach is based on the transmission and measurement of entangled quantum states. First such protocol was proposed by Ekert in 1991 [5]. Later it was shown [3] that an entangled-based protocol may be entirely equivalent to the single-photon BB84 protocol [2] from the viewpoint of the security analysis. That means that the protocol itself may offer information-theoretic (unconditional) key security [3, 12].

A typical implementation of entanglement-based protocol uses a spontaneous down-conversion effect to generate entangled photon pairs. The photons from each pair are delivered to Alice and Bob via two quantum channels. Overall, the implementation of entanglement-based protocols is typically more complicated and expensive than for prepare-and-measure ones. That is why most practical systems rely upon the latter approach. At the same time, entanglement-based protocols offer a number of advantages.

The key advantage is that practically generated entangled photon pairs are completely equivalent to their theoretic model, while single photons in the prepare-and-measure configuration are typically substituted with weak coherent pulses, exhibiting completely different properties. Despite the conventional decoy-state protocols typically provide a feasible solution in the latter case, the system becomes significantly more complex for both the proper implementation and the security analysis. The desire of having a very basic security foundation gives an advantage to the entanglement-based protocols, whose protection essentially rests on the monogamy of entanglement [8]. No matter whether it is a theoretical concept or a practically generated entanglement.

The present paper proposes and discusses a number of approaches to implement entanglement-based QKD protocols

[*] Author to whom any correspondence should be addressed.

as practical tools for key distribution. The central idea is in the optimization of Alice's and Bob's receivers to make them simpler and more practical. This is achieved by means of the active choice of measurement bases. We also propose an active measurement choice solution, that is both simpler and superior in terms of the provided security.

2. Theoretic background

Typically, it is assumed that the entanglement source generates singlet Bell states,

$$|\Psi_0\rangle = \frac{|H\rangle_A|V\rangle_B - |V\rangle_A|H\rangle_B}{\sqrt{2}}, \tag{1}$$

which are invariant under changes of basis. This means that regardless of the measurement basis choice the interlocutors receive fully anti-correlated measurement results, provided the basis is the same for Alice and Bob.

At the same time, in most cases the entangled pair source is connected to the quantum channels via optical fibers, which transform polarization states. These local transformations of the two subsystems modify the original state to a general form, described by the vector

$$|\psi\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} a \\ b \\ b^* \\ -a^* \end{pmatrix}, \tag{2}$$

where $|a|^2 + |b|^2 = 1$ and a star denotes complex conjugation. It is easy to see that this form covers all four Bell states as well as their certain linear combinations.

The same polarization measurements of the two subsystems in (2) in general do not give highly correlated results. However, there exists at least one common measurement basis for Alice and Bob such that they get perfectly correlated outcomes. Unfortunately, this is not enough for QKD, which requires more than one measurement basis.

Conventional protocols may only be implemented in some special cases when $a = 0$ or $b = 0$. In the former one, there are only two viable options for the value of b: either $b = \pm i$ (singlet state) so any measurement basis yields a perfect anti-correlation, or $b = \pm 1$, in which case projections on $(|H\rangle + \exp(i\varphi)|V\rangle)/\sqrt{2}$ ensure an ideal correlation, and measurements in $|H\rangle$—$|V\rangle$ basis give a perfect anti-correlation.

In the latter case any value of a is usable. If $a = \exp(i\theta)$, a perfect anti-correlation appears for projecting on $(|H\rangle + \exp(-i\theta)|V\rangle)/\sqrt{2}$, while a perfect correlation is observed when projected on $\cos\varphi\,|H\rangle + i\sin\varphi\exp(-i\theta)|V\rangle$, where φ is a real number.

In experimental realizations there is typically no way of tracking polarization transformations in fibers, so a polarization controller is blindly employed to achieve required correlations between Alice's and Bob's measurements. This procedure does not reveal the actual two-photon quantum state at the measurement device input. Thus, the state may not be necessary the singlet Bell state.

3. BBM92 protocol

The most straightforward protocol-level implementation of QKD with entangled states was proposed in [3]. The protocol uses two measurement bases comprising of four states: $|H\rangle$, $|V\rangle$, $|D\rangle = (|H\rangle + |V\rangle)/\sqrt{2}$ and $|A\rangle = (-|H\rangle + |V\rangle)/\sqrt{2}$. In later publications [1, 6, 16, 18, 20, 21, 24] researchers elaborated on its actual experimental realization, and came up with a certain polarization measurement scheme, which we will call a passive basis choice. Alice and Bob carry out complete von Neumann measurements in subspaces A and B with polarization beam splitters, while the basis is chosen randomly by a symmetrical beamsplitter (figure 1).

The polarization beamsplitter has one input and two outputs, so it expands the state space: $|\psi\rangle \rightarrow |\psi\rangle_1 \otimes |\psi\rangle_2$. Waveplate only affects the second output component: $|\psi\rangle_1 \otimes |\psi\rangle_2 \rightarrow |\psi\rangle_1 \otimes (\hat{U}|\psi\rangle_2)$, where

$$\hat{U} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}. \tag{3}$$

Therefore, a random state $|\psi\rangle = \alpha|H\rangle + \beta|V\rangle$ is transformed in the following way:

$$|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \xrightarrow{\text{PBS}} \frac{1}{\sqrt{2}}\begin{pmatrix} \alpha \\ \beta \\ \alpha \\ \beta \end{pmatrix} \xrightarrow[\text{plate}]{\text{HW}} \frac{1}{\sqrt{2}}\begin{pmatrix} \alpha \\ \beta \\ (\alpha-\beta)/\sqrt{2} \\ (\alpha+\beta)/\sqrt{2} \end{pmatrix}. \tag{4}$$

The squares of the absolute values of the components of the resulting vector reflect the probabilities of measurement by the detectors H, V, D and A.

The initial state $|\Psi_0\rangle$ (1) is converted to:

$$|\Psi_0\rangle \rightarrow \frac{1}{\sqrt{2}}\left(\begin{pmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ \frac{1}{2} \\ \frac{1}{2} \end{pmatrix}_A \otimes \begin{pmatrix} 0 \\ \frac{1}{\sqrt{2}} \\ -\frac{1}{2} \\ \frac{1}{2} \end{pmatrix}_B - \begin{pmatrix} 0 \\ \frac{1}{\sqrt{2}} \\ -\frac{1}{2} \\ \frac{1}{2} \end{pmatrix}_A \otimes \begin{pmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ \frac{1}{2} \\ \frac{1}{2} \end{pmatrix}_B\right). \tag{5}$$

The resulting state allows us to calculate the probabilities of various measurement outcomes. They are provided in table 1.

After a series of measurements, Alice and Bob discard measurements corresponding to mismatched bases and obtain a common key, losing half of the original sequence. One of the interlocutors should invert the sequence to get closely matching pair of keys.

An obvious disadvantage of this approach is the requirement of having eight single-photon detectors, which makes the experimental setup expensive and much more complex than for the conventional BB84 protocol.

Below we discuss ways of simplifying measurement circuits to reduce the number of detectors. One approach implies an active choice of the measurement basis by means of an electro-optic cell. Another approach is based on time multiplexing, which also helps to reduce the number of detectors.

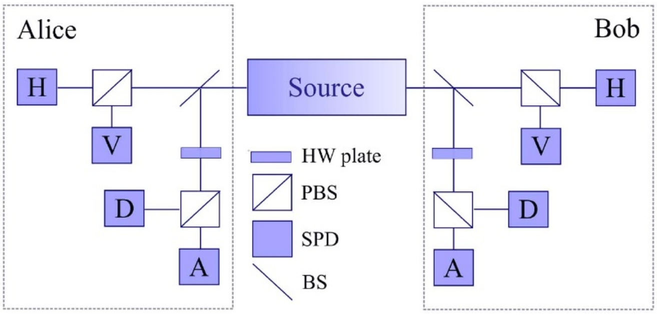

Figure 1. BBM92 circuit with a passive basis choice. PBS—polarizing beamsplitter, SPD—single photon detector, BS—symmetrical beamsplitter.

Table 1. Probabilities P_{AB} of various outcomes for the initial state $|\Psi_0\rangle$.

			Alice			
			H–V		D–A	
			0	1	0	1
Bob	H–V	0	0	$\frac{1}{8}$	$\frac{1}{16}$	$\frac{1}{16}$
		1	$\frac{1}{8}$	0	$\frac{1}{16}$	$\frac{1}{16}$
	D–A	0	$\frac{1}{16}$	$\frac{1}{16}$	0	$\frac{1}{8}$
		1	$\frac{1}{16}$	$\frac{1}{16}$	$\frac{1}{8}$	0

4. Active basis choice

This method was implemented in a number of previous works [4, 7, 23]. According to it, the random selection of the measurement basis is performed by an electro-optic crystal. The crystal operates effectively as a polarization modulator placed before the measurement PBS, as shown in figure 2. Alice and Bob randomly select the modulator state to perform measurements in two mutually unbiased bases, as required by the BBM92 protocol.

In the case of an independent and equiprobable choice of the crystal state for each detected photon, the scheme achieves the same function as the passive one presented before. If the selected bases match, the interlocutors receive a bit of the key. Otherwise, the results of the measurements will be uncorrelated and random.

There is an option to use these uncorrelated and, thus, meaningless measurement results to generate random bits for modulator control. Its practical implementation may rely upon a simple deterministic randomness extractor [9].

As an electro-optic crystal acts effectively as a variable phase plate, its axis orientation plays a crucial role for achieving the goal of basis shifting. To be able to switch to a mutually unbiased basis, the waveplate axis should be oriented at 45° to the principal axes of the PBS. The corresponding rotation matrix can then be written as

$$\hat{U}_\phi = \frac{1}{2}\begin{pmatrix} e^{i\phi}+1 & e^{i\phi}-1 \\ e^{i\phi}-1 & e^{i\phi}+1 \end{pmatrix}. \tag{6}$$

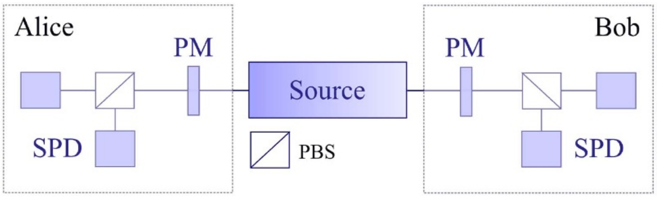

Figure 2. Generic setup for BBM92 with the active basis choice. PM—polarization modulator.

If we assume that no voltage on the electro-optic polarization modulator makes no polarization transformation, to achieve measurements in the circular basis $|R\rangle - |L\rangle$, we need a phase shift of $\pi/2$, which transforms $|H\rangle$ and $|V\rangle$ into

$$|R\rangle = \frac{1}{2}\begin{pmatrix} i+1 \\ i-1 \end{pmatrix}, \qquad |L\rangle = \frac{1}{2}\begin{pmatrix} i-1 \\ i+1 \end{pmatrix}. \tag{7}$$

The initial state (1), depending on the combinations of voltages on the modulators, will be transformed as follows:

$$\phi_A = 0\ [\text{H–V}], \qquad \phi_B = 0\ [\text{H–V}]$$

$$|\Psi_0\rangle \rightarrow |\chi\rangle = \frac{1}{\sqrt{2}}\left(\begin{pmatrix} 1 \\ 0 \end{pmatrix}_A \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix}_B - \begin{pmatrix} 0 \\ 1 \end{pmatrix}_A \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix}_B\right). \tag{8}$$

The probabilities of measuring specific selected bits for Alice and Bob (that is, the probability of receiving clicks from detectors in specific detection windows) are:

$$\begin{aligned} P(A=0,B=0) &= |\langle H_A H_B|\chi\rangle|^2 = 0 \\ P(A=0,B=1) &= |\langle H_A V_B|\chi\rangle|^2 = \frac{1}{2} \\ P(A=1,B=0) &= |\langle V_A H_B|\chi\rangle|^2 = \frac{1}{2} \\ P(A=1,B=1) &= |\langle V_A V_B|\chi\rangle|^2 = 0. \end{aligned} \tag{9}$$

Similar equations can be written for the case when Alice and Bob choose different bases:

$$\phi_A = \pi/2\ [\text{R–L}], \qquad \phi_B = 0\ [\text{H–V}]$$

$$|\chi\rangle = \frac{1}{2\sqrt{2}}\left(\begin{pmatrix} i+1 \\ i-1 \end{pmatrix}_A \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix}_B - \begin{pmatrix} i-1 \\ i+1 \end{pmatrix}_A \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix}_B\right). \tag{10}$$

In this case

$$P(A=0,B=0) = |\langle H_A H_B|\chi\rangle|^2 = \frac{|i-1|^2}{8} = \frac{1}{4}. \tag{11}$$

Other probabilities are calculated in a similar way:

$$\begin{aligned} P(A=0,B=0) &= P(A=0,B=1) = P(A=1,B=0) \\ &= P(A=1,B=1) = \frac{1}{4}. \end{aligned} \tag{12}$$

From the properties of state (1), it can be seen that for the other two options of bases choice, probabilities will be similar to (9) and (12). Since all four options for choosing a phase on modulators are equally likely, the detection probabilities will correspond to table 1.

Here we summarize the possible geometry of the electro-optic crystal and the applied electrical field. We will assume a single-axis crystal that changes optical phase by means of the Pockels effect. The most reliable option is to position the crystal such as the radiation propagates along its axis, so that there is no residual birefringence when the voltage is off. In the opposite case, the large birefringence would lead to detrimental polarization fluctuations due to environmental effects. A crystal in this configuration is typically called Z-cut, as the light propagates along the crystal axis Z.

One of the best electro-optic materials is Lithium Niobate $\mathrm{LiNbO_3}$. So we further assume that we use it as a detailed example. As shown in the appendix the presence of a voltage U applied along H or V axis (assuming Z is horizontal), the crystal develops a birefringence with the fast/slow axes at 45° to H and V. The overall relative phase shift between the fast and slow axes equals

$$\phi = \frac{2\pi L n_o^3 r_{22}}{\lambda d} U, \tag{13}$$

where:
L—crystal length,
n_o—refractive index of ordinary ray,
r_{22}—element of relative dielectric tensor,
λ—wavelength,
d—crystal width between the electrodes.

To estimate the required voltage we assume that $\mathrm{LiNbO_3}$ crystal size is $3 \times 3 \times 20\,\mathrm{mm}^3$ and its long side is along its axis. The working wavelength is 810 nm. Taking other parameters from [22] we can calculate the ratio U/ϕ, which appears to be 0.29 kV. Therefore, for the implementation of BBM92 protocol with the active basis choice one needs a voltage of $U_{\pi/2} \approx 0.45$ kV.

5. Time-multiplexing

One more way of reducing the number of single-photon detectors in the scheme is based on time multiplexing. The general idea is to replace spatial modes that are registered by separate detectors with temporal modes that can be measured by the same detector, but in separate time windows. It has been used in experimental realizations of prepare-and-measure protocols [14, 15]. Although, its use for entangled-based protocols is a bit more involved, due to the lack of an external synchronization signal, it has been also proposed before in [17].

This approach is compatible with both passive [17] and active (see figure 3) basis choice types. The problem of the lack of an external synchronization can be in general solved by using incompatible time delays at Alice's and Bob's sites. Otherwise, the observed coincidence counts will not be able to convey bit value information to the users.

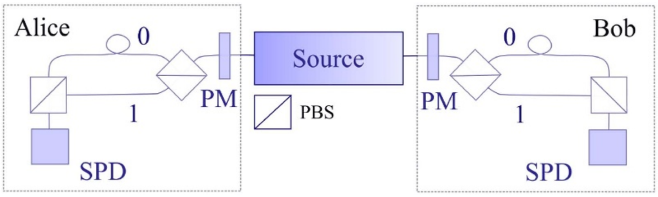

Figure 3. Time-multiplexing realization of the entanglement-based QKD with an active basis choice.

Despite the relative simplicity and the ability to operate with only one single-photon detector per user, time-multiplexing scheme is inherently susceptible to a time-shift attack, described for prepare-and-measure protocols [19]. The ability of Eve to control the arrival times of quantum states to the receiver stations, thus, creates a loophole, compromising the key security. As the scheme is hardwired in such a way that different delays are interpreted as different measurement results, there is inherently no workaround against such an attack.

Therefore, the time-multiplexing-based approach cannot be considered as a promising solution to the problem of reduction the number of detectors.

6. Active projective measurement choice

The studied above active basis choice approach can be further extended to the active choice of not just the measurement basis, but rather the active choice of a projective measurement. In this way the scheme needs only one single-photon detector per user. The basic structure of its realization is shown in figure 4. The polarization modulator provides the required polarization transformations and is followed with a fixed polarizer and a single-photon detector.

For example, in order to implement BBM92 protocol, the interlocutors not only choose a basis ([H–V] or [R–L]) but also a state by randomly choosing between four polarization shifts $\hat{U}_\phi$:

$$\hat{U}_{0^\circ} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad \hat{U}_{180^\circ} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$
$$\hat{U}_{90^\circ} = \frac{1}{2}\begin{pmatrix} i+1 & i-1 \\ i-1 & i+1 \end{pmatrix} \quad \hat{U}_{270^\circ} = \frac{1}{2}\begin{pmatrix} -i+1 & -i-1 \\ -i-1 & -i+1 \end{pmatrix}. \tag{14}$$

The action of the polarizers located after the electro-optical crystals is described by the projectors:

$$\hat{P}_H = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \qquad \hat{P}_V = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \tag{15}$$

$$P_{AB} = \left| \left\langle HV \middle| \hat{U}_{\phi_A} \hat{P}_H \otimes \hat{U}_{\phi_B} \hat{P}_V \middle| \Psi_0 \right\rangle \right|^2. \tag{16}$$

As in the conventional realization of BBM92, the interlocutors discard measurement results corresponding to different bases and keep a bit sequence from matching bases. For example, measurement results at $\phi = 0^\circ$ or 90° are mapped to the bit value of 0, and $\phi = 180^\circ$ or 270° to the value of 1.

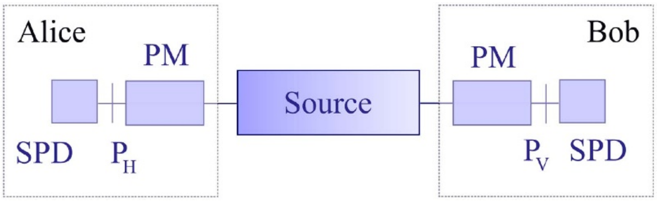

Figure 4. Entanglement-based QKD with the active choice of the projective measurement. P_H and P_V are polarizers oriented along H and V axes.

Table 2. Probabilities of measurement outcomes for the scheme with the active choice of a projective measurement.

			Alice			
			H–V		R–L	
		Phase Shift	0	180	90	270
Bob	H–V	0	$\frac{1}{8}$	0	$\frac{1}{16}$	$\frac{1}{16}$
		180	0	$\frac{1}{8}$	$\frac{1}{16}$	$\frac{1}{16}$
	R–L	90	$\frac{1}{16}$	$\frac{1}{16}$	$\frac{1}{8}$	0
		270	$\frac{1}{16}$	$\frac{1}{16}$	0	$\frac{1}{8}$

Table 2 shows that the probability distribution is similar to the previous schemes. At the same time, the scheme does not open any loopholes with respect with the two-detector active basis choice version. On the contrary, as there is only one detector per user, the detector mismatch vulnerability [13] cannot be exploited in this scenario.

Further, the scheme may be quickly modified to the use of more than two measurement bases. It could be done with a sole change of the electronic drivers for polarization modulators to allow for more than 4 different voltages. A scheme is thus compatible with protocols, based on more than four geometrically uniform states [10, 11].

7. Conclusions

We have studied possible ways of implementing polarization entanglement-based QKD, comparing the conventional passive scheme with a number of alternatives. We proposed an active measurement choice approach, which requires only one single-photon detector per user in contrast to 4 in the passive scheme. Unlike the time-multiplexing detector scheme, this solution does not degrade system security, and on the contrary makes it better by eliminating the threat of the detector-mismatch attack.

Acknowledgment

This work was supported by the contract with JSCo Russian Railways.

Appendix. Electro-optic effect

Consider a lithium niobate crystal cut along the optical Z axis. Light passes along the normal to the xy plane, so there is no birefringence in the absence of an external electric field, $n_x = n_y = n_o$.

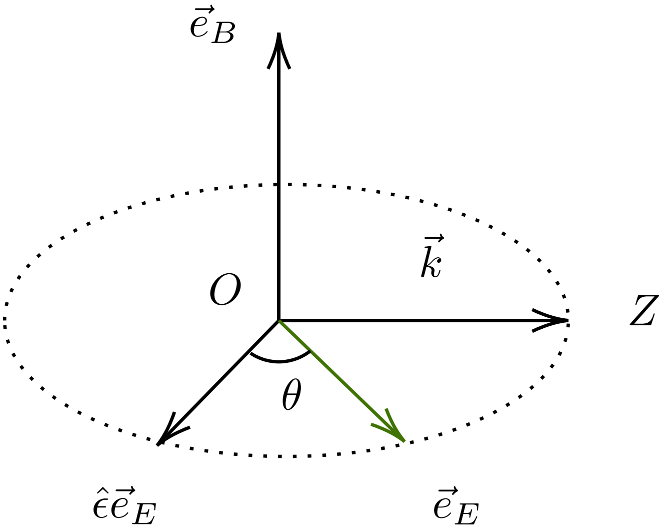

Figure 5. Mutual arrangement of tension and electric induction vectors.

When the field $\vec{E} \uparrow\uparrow \vec{e}_x$ is applied, a linear electro-optic response is observed. Thus, the modified refractive index ellipsoid becomes

$$\left(\frac{1}{n_{ij}^2} + r_{ijk}E_k\right) x_j x_j = 1. \tag{17}$$

For LiNbO$_3$ crystal, the tensor r has the form [22]:

$$r = \begin{pmatrix} 0 & r_{12} & r_{13} \\ 0 & r_{22} & r_{23} \\ 0 & 0 & r_{33} \\ 0 & r_{42} & 0 \\ r_{51} & 0 & 0 \\ r_{61} & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & -r_{22} & r_{13} \\ 0 & r_{22} & r_{13} \\ 0 & 0 & r_{33} \\ 0 & r_{51} & 0 \\ r_{51} & 0 & 0 \\ -r_{22} & 0 & 0 \end{pmatrix}. \tag{18}$$

Wave vector equation

It is convenient to use the following notation, where the key vectors are decomposed onto the amplitudes and corresponding unit vectors:

$$\vec{E} = \vec{e}_E E \quad \vec{B} = \vec{e}_B B \quad \vec{D} = \hat{\epsilon}\vec{e}_E E, \tag{19}$$

where $|\vec{e}_E| = |\vec{e}_B| = 1$. This geometry is shown in figure 5.

From Maxwell's equations, the equation relating the field $\vec{E}$ and the wave vector $\vec{k}$ is:

$$\begin{cases} [\vec{k} \times \vec{e}_E] = \frac{\omega}{c}\frac{B}{E}\vec{e}_B \\ [\vec{k} \times \vec{e}_B] = \frac{\omega}{c}\frac{E}{B}\hat{\epsilon}\vec{e}_E \end{cases} \implies k^2 \cos\theta = \frac{\omega^2}{c^2}|\hat{\epsilon}\vec{e}_E|. \tag{20}$$

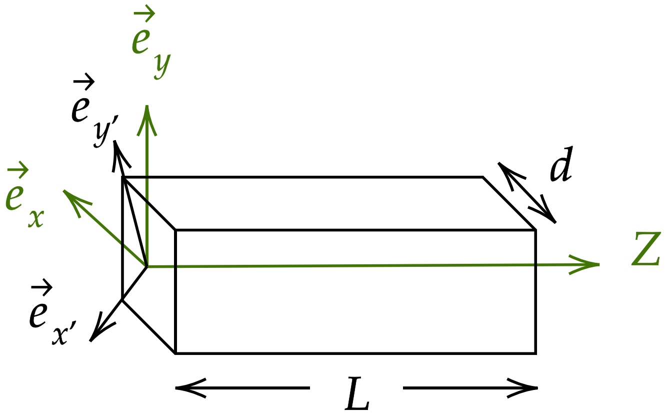

Figure 6. Position of symmetry axes ($\vec{e}_x, \vec{e}_y$) and optical axes ($\vec{e}_{x'}, \vec{e}_{y'}$) of the crystal.

Optical axes arrangement

According to the equation (20):

$$\vec{E} \in \{\vec{e}_z \vec{D}\} \qquad \vec{D} \in \{\vec{e}_x \vec{e}_y\}. \tag{21}$$

When the field is turned on, the crystal becomes biaxial, and the correction to the permittivity tensor equals

$$\hat{\epsilon}^{-1} = \begin{pmatrix} \frac{1}{n_o^2} & -r_{22}E_x & r_{51}E_x \\ -r_{22}E_x & \frac{1}{n_o^2} & 0 \\ r_{51}E_x & 0 & \frac{1}{n_e^2} \end{pmatrix}. \tag{22}$$

The refraction ellipsoid (17) converts to

$$\frac{x^2}{n_x^2} + \frac{y^2}{n_y^2} + \frac{z^2}{n_z^2} + 2r_{51}E_x - 2r_{22}xyE_x = 1. \tag{23}$$

From the relative position of the vectors $\vec{E}$ and $\vec{D}$ one can find the following relations:

$$(\vec{E}, [\vec{k} \times \vec{D}]) = (\hat{\epsilon}^{-1}\vec{D}, [\vec{e}_z \times \vec{D}]) = 0 \tag{24}$$

$$\vec{e}_D = d_x \vec{e}_x + d_y \vec{e}_y \quad [\vec{e}_z \times \vec{D}] = d_y \vec{e}_x - d_x \vec{e}_y. \tag{25}$$

Equations (24) and (25) imply the polarization condition

$$\begin{aligned} d_y(\epsilon_{xx}^{-1} d_x + \epsilon_{xy}^{-1} d_y) &= d_x(\epsilon_{yx}^{-1} d_x + \epsilon_{yy}^{-1} d_y) \\ &\implies d_x = \pm d_y = \pm\frac{1}{\sqrt{2}}. \end{aligned} \tag{26}$$

Consequently, the new directions of polarization correspond to the $\vec{e}_{x'}\vec{e}_{y'}$ axes rotated by 45° with respect to $\vec{e}_x\vec{e}_y$ (figure 6).

Induced phase

Unit vectors $\vec{e}_E$ and $\vec{e}_D$ and the angle between them can be expressed as follows:

$$\begin{aligned} \vec{e}_E = \frac{\hat{\epsilon}^{-1}\vec{e}_D}{|\hat{\epsilon}^{-1}\vec{e}_D|} &\implies |\hat{\epsilon}\vec{e}_E| = \frac{1}{|\hat{\epsilon}^{-1}\vec{e}_D|} \\ \cos\theta = (\vec{e}_E, \vec{e}_D) &= \frac{(\hat{\epsilon}^{-1}\vec{e}_D, \vec{e}_D)}{|\hat{\epsilon}^{-1}\vec{e}_D|}. \end{aligned} \tag{27}$$

Substituting these expressions into equation (20) we obtain two solutions k_1, k_2:

$$k^2 = \frac{\omega^2}{c^2} \frac{1}{(\hat{\epsilon}^{-1}\vec{e}_D, \vec{e}_D)}. \tag{28}$$

$$\begin{aligned} (\hat{\epsilon}^{-1}\vec{e}_D, \vec{e}_D) &= (\epsilon_{xx}^{-1} d_x + \epsilon_{xy}^{-1} d_y) d_x + (\epsilon_{xy}^{-1} d_x + \epsilon_{yy}^{-1} d_y) d_y \\ &= \frac{1}{n_o^2} \pm r_{22}E_x \end{aligned} \tag{29}$$

$$k_{1,2} = \frac{\omega}{c} \frac{1}{\sqrt{\frac{1}{n_o^2} \pm r_{22}E_x}} \approx \frac{\omega}{c} n_o \left(1 \pm \frac{1}{2} n_o^2 r_{22} E_x\right). \tag{30}$$

Therefore, a crystal of length L creates a phase difference between the fast and slow axes equal to:

$$\varphi = L(k_1 - k_2) \approx L\frac{\omega}{c} n_o^3 r_{22} E_x. \tag{31}$$

Phase shift

Let us now consider propagation of a linearly polarized light through the crystal. Denote the input polarization vector

$$\vec{E} = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}. \tag{32}$$

The transition to the coordinates of the optical axes of the crystal $\vec{e}_x, \vec{e}_y$ is carried out using the rotation matrix $\hat{M}$, while the action of the crystal itself is described by the matrix Λ_ϕ:

$$\hat{M} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}, \qquad \hat{\Lambda}_\phi = \begin{pmatrix} e^{i\phi} & 0 \\ 0 & 1 \end{pmatrix}. \tag{33}$$

After passing through the crystal, the initial vector (32) transforms into:

$$\vec{E} \to \hat{M}^{-1} \Lambda_\phi \hat{M} \vec{E} = \frac{1}{2} \begin{pmatrix} e^{i\phi} + 1 & e^{i\phi} - 1 \\ e^{i\phi} - 1 & e^{i\phi} + 1 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix}. \tag{34}$$

A simple check shows that for the states $|H\rangle$ ($\alpha = 1, \beta = 0$) and $|V\rangle$ ($\alpha = 0$, $\beta = 1$) the phase shift π gives a linear polarization orthogonal to the input, while $\phi = \pm\pi/2$ gives a circular polarization.

References

[1] Basset F B *et al* 2021 Quantum key distribution with entangled photons generated on demand by a quantum dot *Sci. Adv.* **7** eabe6379

[2] Bennett C H and Brassard G 1984 Quantum cryptography: public key distribution and coin tossing *Proc. IEEE Int. Conf. on Computers, Systems and Signal Processing* (Bangalore) pp 175–9

[3] Bennett C H, Brassard G and Mermin N D 1992 Quantum cryptography without Bell's theorem *Phys. Rev. Lett.* **68** 557–9

[4] Cao Y *et al* 2013 Entanglement-based quantum key distribution with biased basis choice via free space *Opt. Express* **21** 27260–8

[5] Ekert A 1991 Quantum cryptography based on Bell's theorem *Phys. Rev. Lett.* **67** 661–3

[6] Erven C, Couteau C, Laflamme R and Weihs G 2008 Entangled quantum key distribution over two free-space optical links *Opt. Express* **16** 16840–53

[7] Jennewein T, Simon C, Weihs G, Weinfurter H and Zeilinger A 2000 Quantum cryptography with entangled photons *Phys. Rev. Lett.* **84** 4729–32

[8] Koashi M and Winter A 2004 Monogamy of quantum entanglement and other correlations *Phys. Rev.* A **69** 022309

[9] Kravtsov K, Radchenko I, Kulik S and Molotkov S 2015 Minimalist design of a robust real-time quantum random number generator *J. Opt. Soc. Am.* B **32** 1743

[10] Kravtsov K S and Molotkov S N 2019 Practical quantum key distribution with geometrically uniform states *Phys. Rev.* A **100** 042329

[11] Kravtsov K S and Molotkov S N 2021 Reply to "Comment on 'Practical quantum key distribution with geometrically uniform states' " *Phys. Rev.* A **104** 026402

[12] Ma X, Fung C-H F and Lo H-K 2007 Quantum key distribution with entangled photon sources *Phys. Rev.* A **76** 012307

[13] Makarov V, Anisimov A and Skaar J 2006 Effects of detector efficiency mismatch on security of quantum cryptosystems *Phys. Rev.* A **74** 022313

[14] Makarov V, Brylevski A and Hjelme D R 2004 Real-time phase tracking in single-photon interferometers *Appl. Opt.* **43** 4385–92

[15] Marand C and Townsend P D 1995 Quantum key distribution over distances as long as 30 km *Opt. Lett.* **20** 1695–7

[16] Marcikic I, Lamas-Linares A and Kurtsiefer C 2006 Free-space quantum key distribution with entangled photons *Appl. Phys. Lett.* **89** 101122

[17] Peev M and Bettelli S 2012 QKD arrangement *US Patent* 8,189,966

[18] Poppe A *et al* 2004 Practical quantum key distribution with polarization entangled photons *Opt. Express* **12** 3865–71

[19] Qi B, Fung C-H, Lo H-K and Ma X 2007 Time-shift attack in practical quantum cryptosystems *Quantum Info. Comput.* **7** 73–82

[20] Shi Y, Moe Thar S, Poh H S, Grieve J A, Kurtsiefer C and Ling A 2020 Stable polarization entanglement based quantum key distribution over a deployed metropolitan fiber *Appl. Phys. Lett.* **117** 124002

[21] Weihs G and Erven C 2007 Entangled free-space quantum key distribution *Proc. SPIE* **6780** 678013

[22] Weis R S and Gaylord T K 1985 Lithium niobate: summary of physical properties and crystal structure *Appl. Phys.* A **37** 191–203

[23] Yin J *et al* 2017 Satellite-to-ground entanglement-based quantum key distribution *Phys. Rev. Lett.* **119** 200501

[24] Yin J *et al* 2020 Entanglement-based secure quantum cryptography over 1,120 kilometres *Nature* **582** 501–5