Eur. Phys. J. D **42**, 139–145 (2007)
DOI: 10.1140/epjd/e2006-00279-7

THE EUROPEAN PHYSICAL JOURNAL D

Simulating phase coding in quantum cryptography: influence of chromatic dispersion

M. Suda[1,a], T. Herbst[2], and A. Poppe[3]

[1] ARC Seibersdorf research GmbH, Tech Gate Tower, Donau-City-Str. 1, 1220 Wien, Austria
[2] Technische Universität Wien, Karlsplatz 13, 1040 Wien, Austria
[3] Institut für Experimentalphysik, Universität Wien, Boltzmanngasse 5, 1090 Wien, Austria

Received 28 August 2006 / Received in final form 9 October 2006
Published online 22 December 2006 –

Abstract. We demonstrate the impact of chromatic dispersion on the phase coding method in a double Mach-Zehnder implementation of an interferometric system for quantum cryptography. Formulas have been developed to explore detailed studies of the modifications on energy and position spectra which arise if chromatic dispersion is taken into account. Examples demonstrate the shifting of spectra and the appearance of oscillations depending on the wavelength and spectral broadness as well as on the phase shifters, absorbers and the dimensions of the interferometric set-up.

PACS. 03.67.Dd Quantum cryptography – 03.67.Hk Quantum communication

QICS. 23.05.+f Fiber-based quantum communication

1 Introduction

Chromatic dispersion (CD) plays an important role in interferometers, that can be established with single-mode optical fiber components for quantum key distribution (QKD) using phase coding [1,2]. Originally, the phase coding method with optical fibers and a single Mach-Zehnder interferometer (MZ) was introduced (see Fig. 1) together with entanglement-based quantum cryptography [3], but it can also be used with the single-particle schemes. In order to record stationary interferences, it unfortunately is very difficult to keep the path difference stable (necessary for QKD) in such an extended interferometer (each arm should be several tenth of kilometers).

Therefore a better practical set-up consists of 2 unbalanced MZ [4], shown in Figure 2. Figures 1 and 2 are discussed in more detail in Sections 4 and 5. These 2 interferometers are connected in series by a single optical fiber (fiber g in Fig. 2). The first Mach-Zehnder interferometer (1.MZ) on the left side belongs to Alice (A) and the second Mach-Zehnder interferometer (2.MZ) on the right side belongs to Bob (B), the two communication partners. One pulse entering Alice's side (input a) is split into two. The two pulses propagating one after the other along the single transmission fiber g are denoted by S (for short path) and L (for long path). If the path differences in both interferometers are different, four pulses are created after traveling through Bob's 2.MZ. But if the path differences are equal, only 3 pulses are created. That case is indicated schematically in Figure 2. Two of them, noted SS (short-short) and LL (long-long), are not relevant, as they show no interference effect. The central pulse, however, corresponds to two possible paths: SL or LS, which are indistinguishable and which therefore interfere. The choice of the phase shifts by A and B gives the encoding-decoding. A timing window can be used to distinguish between interfering and non-interfering events. This set-up is much more stable than the original one, since the pulses actually follow the same path g. The disturbances due to environmental perturbations like length variations affect both positions of the photons equally. Therefore, the path lengths of the single interferometers should be small in comparison to the length of the fiber g in between.

We recognize that the imbalance of the interferometers must be chosen in such a way that it is possible to clearly distinguish the three spatial (or temporal) peaks and thus discriminate interfering from non-interfering events. It is known that CD displaces and broadens these peaks. In that case, CD can cause problems for quantum cryptography. For instance, schemes implementing phase- or phase-and-time-coding rely on photons arriving at well-defined times, that is on photons well localized in space. However, in dispersive media like optical fibers, different group velocities act as a noisy environment on the localization of the photon as well as on the phase acquired in an interferometer. Hence, the broadening of photons featuring non-zero bandwidth must be circumvented or controlled. This implies working with photons of small bandwidth, or, as long as the bandwidth is not too large, operating close to the wavelength where CD is zero, i.e. for standard fibers around 1312 nm. There are also special fibers, called

[a] e-mail: martin.suda@arcs.ac.at

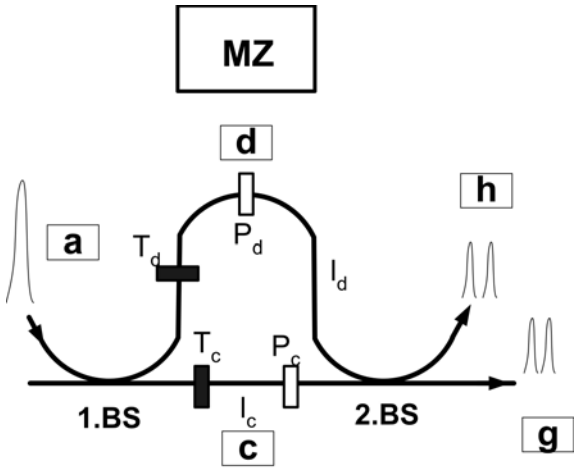

Fig. 1. MZ interferometer: 1 input a, 2 outputs h, g, 2 beam splitters (BS), 2 optical fibers ($i = c, d$), fiber lengths l_i, phase factors $P_i = \exp\{-\imath k \Delta_i\}$, Δ_i are phase shifters, transmission coefficients $T_i = \exp\{-2 l_i a_i\}$ (a_i are absorption factors); position distributions (or time pulses) are drawn.

dispersion-shifted, with a refractive index profile which causes the CD to go to zero around 1550 nm. Methods of dispersion compensation or filtering are therefore applied [5,6]. CD becomes a serious issue depending on the used bandwidth of the photons. Utilizing photon pairs created by spontaneous parametric down-conversion $SPDC$ ($\delta\lambda \approx 10$ nm, corresponding to 1.2×10^3 GHz) is more critical than faint laser pulses with pulsed diodes with a width of 10 to 100 GHz or more. We will show that even the latter sources are heavily disturbed by CD.

From the considerations above it can be assumed that a detailed description of the processes, which arise if CD comes into play, could be of fundamental interest to the specialist dealing with fiber optics and phase-coding systems using MZ interferometers in quantum cryptography. It is the intention of this paper to theoretically investigate in detail the effects which appear, if CD in two MZ interferometers in series is taken into account. Using Gaussian wave packets, formulas are developed which describe both, wavelength spectra and position spectra, arising in a double MZ implementation of an interferometric system for quantum cryptography.

The paper is organized as follows: in Section 2 the wave packet description is shortly presented. In Section 3 CD is introduced. The action of the two beam splitters in an interferometer is specified in Section 4, whereas in Section 5 the double MZ-System is analyzed. Section 6 presents results and discussions of an instructive example and finally, in Section 7, conclusions are drawn.

2 Wave packet description

We are investigating one incoming beam, let us say a beam in path a (Fig. 1). The basic approach for the momentum of photons of this incoming beam in path a is given according to a Gaussian function

$$\alpha_a(k) = [2\pi(\delta k)^2]^{-1/4} \exp\left\{-\frac{(k-k_0)^2}{4(\delta k)^2}\right\}, \qquad (1)$$

where the normalization condition for the intensity $I_a = \int \alpha_a^2(k) dk = 1$ holds (integration boundaries are always $-\infty$ to $+\infty$). The wave number k is associated with the wave length λ via the equation $k = 2\pi/\lambda$. The relation $p = \hbar k$ connects the momentum p and wave number k. A mean wave number $k_0 > 0$ is important for describing an experimental wave length distribution. The corresponding wave function $\psi_a(x)$ is given by Fourier transformation and reads as

$$\begin{aligned}\psi_a(x) &= \frac{1}{\sqrt{2\pi}} \int \alpha_a(k) \exp\{ikx\} dk \\ &= \left[\frac{2(\delta k)^2}{\pi}\right]^{1/4} \exp\{-(\delta k)^2 x^2 + \imath k_0 x\}, \qquad (2)\end{aligned}$$

where $(\delta k)^2$ is the mean square deviation of wave numbers. The suitable momentum and position spectra are calculated as

$$\alpha_a^2(k) = \sqrt{\frac{1}{2\pi(\delta k)^2}} \exp\left\{-\frac{(k-k_0)^2}{2(\delta k)^2}\right\} \qquad (3)$$

and

$$|\psi_a(x)|^2 = \sqrt{\frac{2(\delta k)^2}{\pi}} \exp\{-2(\delta k)^2 x^2\} \qquad (4)$$

respectively. Again, the normalization condition for intensity can be written as $I_a = \int |\psi_a(x)|^2 dx = 1$. The momentum spectrum $\alpha_a^2(k)$ is an experimental quantity. A Gaussian spectrum is definitely an idealization, but a very reasonable and even realistic one. The advantage of Gaussian shaped momentum and position spectra is mainly given by mathematical simplicity of the formalism and by the easy interpretation of the results.

3 Chromatic dispersion (CD)

There are two arms c and d in the first Mach-Zehnder (MZ) interferometer and two outputs g and h (Fig. 1). Initially we assume a MZ in vacuum. It follows that, on the one hand, the beam paths c and d are characterized by path lengths l_c and l_d giving rise to phase factors $e^{-\imath k l_c}$ and $e^{-\imath k l_d}$ respectively. On the other hand, phase shifts Δ_c and Δ_d create phase factors $P_c = e^{-\imath k \Delta_c}$ as well as $P_d = e^{-\imath k \Delta_d}$. Finally, absorption factors a_c and a_d entail transmission coefficients $T_c = e^{-2 l_c a_c}$ and $T_d = e^{-2 l_d a_d}$ to be included if desired. These transmission factors have to be functions of the lengths of the absorbers to be considered.

Since the group velocity v and the coefficient D_{λ_0} of CD are the most important parameters governing pulse propagation in dispersive media like fiber glass, it is necessary to examine their dependence on the wavelength [7]:

$$v = \frac{c_0}{N}, \quad N = n - \lambda \frac{dn}{d\lambda}, \qquad (5)$$

Table 1. Dispersion coefficients D_{λ_0} and the parameter $\kappa = -D_{\lambda_0}\lambda_0^2 c_0/(4\pi)$ for 3 particular wavelength λ_0 [7].

λ_0[nm]	$D_{\lambda_0}\left[\frac{\text{ps}}{\text{km nm}}\right]$	κ[nm]
870	–80	1.4456
1312	0	0
1550	17	–0.3072

where c_0 is the light velocity in vacuum, $n = n(\lambda)$ is the refractive index and $N = N(\lambda)$ is called group index. Including CD, it can be shown that in a fiber glass of length l the phase factor $\exp\{-\imath kl\}$ has to be replaced by $\exp\{-\imath(N_0 k - \kappa k^2)l\}$, where $N_0 = N(\lambda_0)$ is the group index for the mean wavelength λ_0 and $\kappa = -D_{\lambda_0}\lambda_0^2 c_0/(4\pi)$. Caused by CD, the exponential function is extended by an expression which is proportional to k^2. Thereby the dispersion coefficient is defined through

$$D_{\lambda_0} = -\frac{\lambda_0}{c_0}\left.\frac{\partial^2 n}{\partial\lambda^2}\right|_{\lambda=\lambda_0}. \tag{6}$$

Table 1 presents some dispersion coefficients D_{λ_0} and $\kappa-$values for three distinguished wavelengths λ_0.

4 Calculation of spectra behind the first MZ

Here we proceed describing the action of beam splitters [8] and the superposition of wave packets as formulated in [9]. The corresponding picture is drawn in Figure 1. The total phase factor in a fiber of length l_j is given by

$$\exp[-\imath kA_j - \imath k^2 B_j], \quad A_j = \Delta_j + N_0 l_j, \quad B_j = \kappa l_j, \quad j = c, d. \tag{7}$$

The properties of a 50:50 beam splitter BS can be described by the Hadamard transformation $\hat{H}$:

$$\hat{H} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \tag{8}$$

If only one input (beam a) exists, the wave number functions $\alpha_{d,c}(k)$ in the two beam paths d and c directly in front of the second BS are given by

$$\alpha_{d,c}(k) = \frac{1}{\sqrt{2}}\,\alpha_a(k)\sqrt{T_{d,c}}\,\exp[-\imath kA_{d,c} - \imath k^2 B_{d,c}]. \tag{9}$$

Consequently, the wave number functions behind the MZ are

$$\alpha_{h,g}(k) = \hat{H}\alpha_{d,c}(k) = \frac{1}{\sqrt{2}}[\alpha_d(k) \pm \alpha_c(k)]. \tag{10}$$

The related wave number spectra immediately behind the first MZ are therefore

$$|\alpha_{h,g}(k)|^2 = \frac{1}{4}\alpha_a^2(k)\{T_d + T_c \pm 2\sqrt{T_d T_c}\cos[k(A_d - A_c) + k^2(B_d - B_c)]\}. \tag{11}$$

Because of CD, a quadratic term in the argument of the cosine appears, indicating higher frequencies depending on the length of the fiber. By Fourier transformation of (9) the position wave functions $\psi_{d,c}(x)$ become after some calculation

$$\psi_{d,c}(x) = \sqrt{\frac{(\delta k)T_{d,c}}{\sqrt{2\pi}}}\,\frac{1}{\sqrt{1+\imath 4(\delta k)^2 B_{d,c}}} \times \exp\left\{-\frac{1}{\frac{1}{4(\delta k)^4} + 4B_{d,c}^2}\left[\frac{1}{(\delta k)^2}\left[k_0 B_{d,c} + \frac{(A_{d,c}-x)}{2}\right]^2 + \imath\frac{k_0}{4(\delta k)^4}(A_{d,c}-x) + \imath B_{d,c}\left[\frac{k_0^2}{4(\delta k)^4} - (A_{d,c}-x)^2\right]\right]\right\}. \tag{12}$$

Behind the first MZ the position wave functions of both directions d and c become

$$\psi_{h,g}(x) = \hat{H}\psi_{d,c}(x) = \frac{1}{\sqrt{2}}[\psi_d(x) \pm \psi_c(x)]. \tag{13}$$

Hence the corresponding position spectra are

$$|\psi_{h,g}(x)|^2 = \frac{1}{2}[|\psi_d(x)|^2 + |\psi_c(x)|^2 \pm I(x)]. \tag{14}$$

The single quantities are carried out below:

$$\begin{aligned}
|\psi_{d,c}(x)|^2 &= T_{d,c}\frac{(\delta k)}{\sqrt{2\pi\omega_{d,c}}} \times \exp\left\{-\frac{2(\delta k)^2}{\omega_{d,c}}\,[(A_{d,c}-x) + 2k_0 B_{d,c}]^2\right\},\\
\omega_{d,c} &= 1 + 16(\delta k)^4 B_{d,c}^2,\\
I(x) &= \psi_d(x)\psi_c(x)^* + \psi_d(x)^*\psi_c(x)\\
&= c_{dc}\,e_d\,e_c\,\cos(a_d - a_c + a_{dc}),\\
c_{dc} &= \sqrt{T_d T_c}\sqrt{\frac{2}{\pi}}(\delta k)\frac{1}{(\omega_d\omega_c)^{1/4}},\\
e_{d,c} &= \exp\left\{-\frac{4(\delta k)^2}{\omega_{d,c}}\left[k_0 B_{d,c} + \frac{(A_{d,c}-x)}{2}\right]^2\right\},\\
a_{d,c} &= \frac{1}{\omega_{d,c}}\{k_0(A_{d,c}-x) + B_{d,c}[k_0^2 - 4(\delta k)^4(A_{d,c}-x)^2]\},\\
a_{dc} &= \frac{1}{2}\arctan\left[\frac{4(\delta k)^2(B_d - B_c)}{1 + 16(\delta k)^4 B_d B_c}\right].
\end{aligned}$$

From this equation it can be observed that through $\omega_{d,c}$ or rather through $B_{d,c}$ the pulses become broader as a function of the length of the fiber. This limits the process of phase coding in quantum cryptography as we will see below.

According to [5], the quantity $\omega_{d,c}$ can be expressed as ($\delta k = 2\pi(\delta\lambda)/\lambda_0^2$)

$$\omega_{d,c} = 1 + 16\pi^2\left(\frac{c_0}{\lambda_0}\right)^2\left(\frac{\delta\lambda}{\lambda_0}\right)^2[\Delta\tau_{d,c}]^2, \quad \Delta\tau_{d,c} = (\delta\lambda)D_{\lambda_0}l_{d,c}. \tag{15}$$

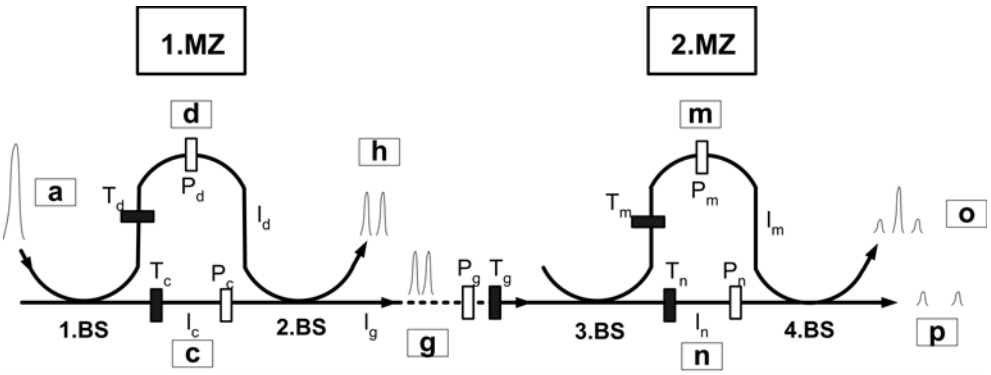

Fig. 2. Two MZ interferometers in series: 1 input a, 3 outputs h, o, p, 4 beam splitters (BS), 5 optical fibers ($i = c, d, g, m, n$), fiber lengths l_i, phase factors $P_i = \exp\{-\imath k \Delta_i\}$, Δ_i are phase shifters, transmission coefficients $T_i = \exp\{-2 l_i a_i\}$ (a_i are absorption factors); position distributions (or time pulses) are drawn.

The Gaussian uncertainty in time due to CD is then defined by the dispersion time $\Delta\tau_{d,c}$. If the dispersion coefficient D_{λ_0} is zero, no broadening of the Gaussian position spectra $|\psi_{d,c}(x)|^2$ appears.

5 Spectra behind the second MZ

As a next step, we analyze two MZ interferometers as depicted in Figure 2. The second interferometer is composed of the third and fourth beam splitter and has two arms m and n as well as two outputs o and p. The single input for this second MZ is fiber g. At the end of this fiber, i.e. directly in front of the 3. BS, the following wave function $\alpha'_g(k)$ can be specified:

$$\alpha'_g(k) = \sqrt{T_g}\alpha_g(k)\exp\{-\imath k A_g - \imath k^2 B_g\}. \quad (16)$$

Here analogue to (9) the transmission coefficient T_g, the phase quantity A_g and the dispersion quantity B_g in fiber g have been specified. Inside the second MZ interferometer but just before the 4. BS the related wave functions read

$$\alpha_{m,n}(k) = \frac{1}{\sqrt{2}}\sqrt{T_{m,n}}\,\alpha'_g(k)\exp\{-\imath k A_{m,n} - \imath k^2 B_{m,n}\}, \quad (17)$$

and on exit of the second interferometer the wave number functions are

$$\alpha_{o,p}(k) = \hat{H}\alpha_{m,n}(k) = \frac{1}{\sqrt{2}}[\alpha_m(k) \pm \alpha_n(k)], \quad (18)$$

and therefore the wave number spectra $|\alpha_{o,p}(k)|^2$ behind the two interferometers can be written as

$$|\alpha_{o,p}(k)|^2 = \frac{1}{4}|\alpha_g(k)|^2 T_g\{T_m + T_n \mp 2\sqrt{T_m T_n}\cos[k(A_m - A_n) + k^2(B_m - B_n)]\} \quad (19)$$

with $|\alpha_g(k)|^2$ from (11) and $k = 2\pi/\lambda$. Now, just as well as above, we use Fourier transformation of $\alpha_{o,p}(k)$ in order to get the position wave functions $\psi_{o,p}(x)$ in direction o and p. The result is:

$$\psi_{o,p}(x) = \frac{1}{4}\frac{1}{\sqrt{2\pi}}\sqrt{T_g}[2\pi(\delta k)^2]^{-1/4} \times \{J_{dm}(x) - J_{cm}(x) \mp J_{dn}(x) \pm J_{cn}(x)\}. \quad (20)$$

The upper sign applies to output o and the lower sign applies to output p. Here the complex quantities $J_{ij}(x)$ are ($ij \equiv dm, cm, dn, cn$)

$$\begin{aligned} J_{ij}(x) &= c_{ij}\sqrt{T_i T_j}\exp\left\{\frac{\imath + 4(\delta k)^2\delta_{ij}}{\gamma_{ij}} \times[-\delta_{ij}k_0^2 + x'_{ij}k_0 + \imath(\delta k)^2 x'^2_{ij}]\right\}, \\ c_{ij} &= \sqrt{\frac{4\pi(\delta k)^2}{1 + \imath 4(\delta k)^2\delta_{ij}}}, \quad \delta_{ij} = B_g + B_i + B_j, \\ x'_{ij} &= x - A_g - A_i - A_j, \\ \gamma_{ij} &= 1 + 16(\delta k)^4\delta_{ij}^2. \end{aligned} \quad (21)$$

Finally, the position spectra are obtained:

$$|\psi_{o,p}(x)|^2 = \frac{T_g}{32\pi\sqrt{2\pi}(\delta k)}\{|J_{dm}(x)|^2 + |J_{cm}(x)|^2 + |J_{dn}(x)|^2 + |J_{cn}(x)|^2 + 2II_{o,p}(x)\}, \quad (22)$$

where

$$\begin{aligned} II_{o,p}(x) = &-\Re[J_{dm}(x)J^*_{cm}(x)] \mp \Re[J_{dm}(x)J^*_{dn}(x)] \\ &\pm\Re[J_{cm}(x)J^*_{dn}(x)] \pm \Re[J_{dm}(x)J^*_{cn}(x)] \\ &\mp\Re[J_{cm}(x)J^*_{cn}(x)] - \Re[J_{dn}(x)J^*_{cn}(x)]. \end{aligned} \quad (23)$$

Figuring out the above expressions we obtain:

$$\begin{aligned} |J_{ij}(x)|^2 &= 4\pi(\delta k)^2\sqrt{\frac{1}{\gamma_{ij}}}T_i T_j \times \exp\{-2(\delta k)^2[x'_{ij} - 2\delta_{ij}k_0]^2/\gamma_{ij}\}, \\ \Re[J_{ij}(x)J^*_{kl}(x)] &= c'_{ij}(x)c'_{kl}(x)\cos[z_{ij}(x) - z_{kl}(x)], \\ c'_{ij}(x) &= 2(\delta k)\sqrt{\pi}\sqrt{T_i T_j}(\gamma_{ij})^{-1/4} \times \exp\{-2(\delta k)^2[x'_{ij} - \delta_{ij}k_0]^2/\gamma_{ij}\}, \\ z_{ij}(x) &= \frac{1}{2}\arctan[4\delta_{ij}(\delta k)^2] + \frac{1}{\gamma_{ij}}[k_0^2\delta_{ij} - k_0 x'_{ij} - 4(\delta k)^4\delta_{ij}x'^2_{ij}]. \end{aligned} \quad (24)$$

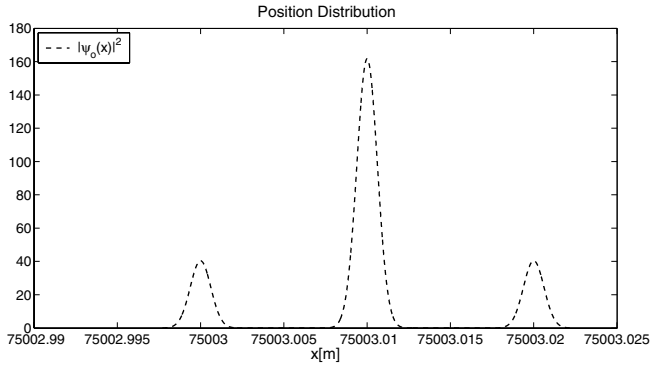

Fig. 3. Without CD and absorption, $l_g = 50\,\text{km}$, $\Delta_d = \Delta_m = 1$ cm, $l_d = l_c = l_m = l_n = 1\,\text{m}$, $\delta\lambda/\lambda_0 = 2 \times 10^{-4}$, $\lambda_0 = 1550$ nm, $N_0 = 1.5$, $\Delta_c = \Delta_g = \Delta_n = 0$.

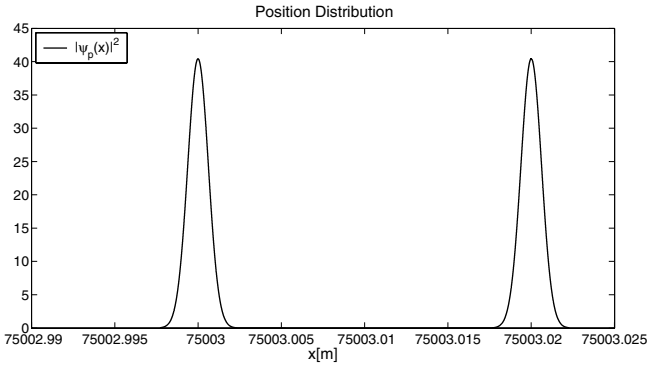

Fig. 4. Same parameters as in Figure 3; please observe the different ordinate scales. The side wings in Figure 3 are exactly the same as the two peaks here.

The quantity $\gamma_{i,j}$ is again responsible for the broadness of the Gaussian functions. But in this case, the sum $\delta_{i,j} = B_g + B_i + B_j$ depends on the length l_g of the fiber ($B_g = \kappa l_g$) between the two interferometers. This length can be very large in quantum key distribution using phase coding methods. We return to this point in the next section.

In the next section, these spectra are displayed using certain parameters demonstrating the influence of chromatic dispersion in the process of phase coding in quantum cryptography.

6 Results and discussion

By means of some examples, the influence of CD on the position and wavelength spectra is illustrated.

Figures 3 and 4 exemplify position distributions $|\psi_o(x)|^2$ and $|\psi_p(x)|^2$ of (22), behind the two interferometers shown in Figure 2, including parameters given in the figure capture. In this example no CD (and no absorption) is considered. The arms of the two interferometers have equal lengths of 1 m each and in arm d and m equal values of phase shifts $\Delta_d = \Delta_m = 1$ cm entail phase factors $P_d = \exp\{-\imath k \Delta_d\}$ and $P_m = \exp\{-\imath k \Delta_m\}$, respectively. These phase shifts are sufficient to create separated wave packets in space (or time pulses) behind the two interferometers which are connected by a fiber of length $l_g = 50$ km, if no dispersion (and no absorption) is taken into account.

Two remarks:

(1) The phase shifts Δ_d and Δ_m easily could be substituted by enlargements of the corresponding lengths of the fibers. This signifies that the phase shifts depend on the group index as well as on the dispersion coefficient.

(2) Another short remark should be made here which is valid for all figures relating to position distributions below as well: the $x-$ scale denotes the distance the photon has to cover as if it would travel in vacuum. Because of the group index the photon needs therefore more time to travel ($t = x/c_0$) in a glass fiber of a certain length than in vacuum, it is slower, of course.

The 2 side peaks, which appear in Figure 3 are due to the fact that the photons take the short arms in each of the two interferometers or propagate through the long arms respectively (i.e. the arms with the phase shifters Δ_d and Δ_m). Therefore, these two side peaks are separated from each other by a value of $\Delta_d + \Delta_m = 2$ cm. The mean position values x_l and x_r, due to the left and right peaks, come from $x_l = (l_g + l_c + l_n)N_0 = 50002 \times 1.5 = 75003$ m and $x_r = (l_g + l_d + l_m)N_0 + \Delta_d + \Delta_m = 75003.02$ m, respectively. These are the mean (hypothetical) distances the photons have to cover, if the short-short and long-long processes are taken into account and if the photons have the vacuum speed of light. Output o in Figure 3 exhibits an additional peak in between, which is four times as large. This is only true if $\Delta_d = \Delta_m$. The short-long and long-short processes are indistinguishable and give rise to constructive interference in this case. In the other beam p (Fig. 4) destructive interference occurs due to the phase factor of the Hadamard transformation of the beam splitter and hence no peak in between appears. The full width of half maximum (FWHM) can be calculated via

$$(\delta x) = \frac{1}{2(\delta k)} = \frac{1}{4\pi}\frac{\lambda_0}{(\delta\lambda)}\lambda_0,$$
$$FWHM = \sqrt{8\ln 2}\,(\delta x) \approx 0.00145\ \text{m} \qquad (25)$$

using $\lambda_0 = 1550$ nm and $\delta\lambda/\lambda_0 = 2 \times 10^{-4}$. Because of the complete separation of the pulses, phase coding can be executed perfectly. However, this case is hypothetical because CD has been omitted.

The corresponding $\lambda-$distribution functions $|\alpha_{o,p}(\lambda)|^2$ can be calculated according to equations (19) and (11) and are drawn in Figure 5. Because of photon conservation, we have $\alpha_a^2(\lambda) = |\alpha_h(\lambda)|^2 + |\alpha_o(\lambda)|^2 + |\alpha_p(\lambda)|^2$, where the envelope in Figure 5 is the input function (3). The distributions are depicted as functions of the wavelength $\lambda = 2\pi/k$ which is more commonly used for presentation. Because of the 2 phase shifts the wavelength spectra get distinct oscillatory structures indicating separation of wave packets in space (or time). For comparison only, the spectrum $|\alpha_h(\lambda)|^2$ of the output port h is drawn as well.

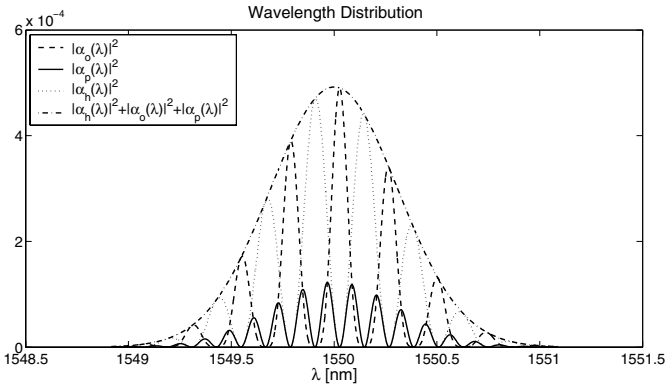

Fig. 5. $\delta\lambda/\lambda_0 = 2 \times 10^{-4}$, $\lambda_0 = 1550$ nm.

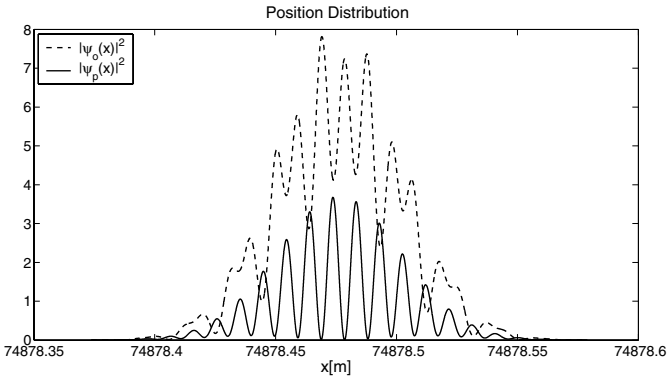

Fig. 6. With CD: $\kappa = -0.3072$ nm for $\lambda_0 = 1550$ nm, $l_g = 50$ km.

Note that separation of wave packets in space entail energy spectra of an oscillatory behavior as seen in Figure 5.

Figure 6 presents the position distributions of the output modes o and p, with the only major difference of including CD for $\lambda_0 = 1550$ nm, which means including a κ of -0.3072 nm according to Table 1 in Section 3. Including CD supplies a much more realistic representation than before (Figs. 3 and 4). It will be shown below that the including of CD is absolutely necessary. The quantity κ comes into play via $B_g = \kappa l_g$ and hence becomes important for large fiber lengths like $l_g = 50$ km in this case. As can be seen, a completely different picture of position distributions, in comparison to Figures 3 and 4, appears in Figure 6. First of all, the spectra are shifted to smaller $x-$values by about 124.5 m. This comes from formulas (24) and (21), where it can be seen that the shifting amounts to $2\kappa k_0(l_g + l_c + l_n)$. Secondly, the region has been broadened from 2 cm in Figures 3 and 4 to about 15 cm in Figure 6. This is discussed below more precisely. And thirdly, both spectra, $|\psi_o(x)|^2$ and $|\psi_p(x)|^2$, exhibit heavily oscillations. The frequency of these modulations is given by the interference terms in (23) and (24). As can be seen there, the modulations depend on the quantity $z_{ij}(x)$ in the argument of the cosine. Because of the relatively large value of $l_g = 50$ km, δ_{ij} becomes large entailing large frequencies. Likewise, these modulations depend on κ as it is shown in the equations mentioned above. Hence, in this case, it is completely impossible to execute phase coding.

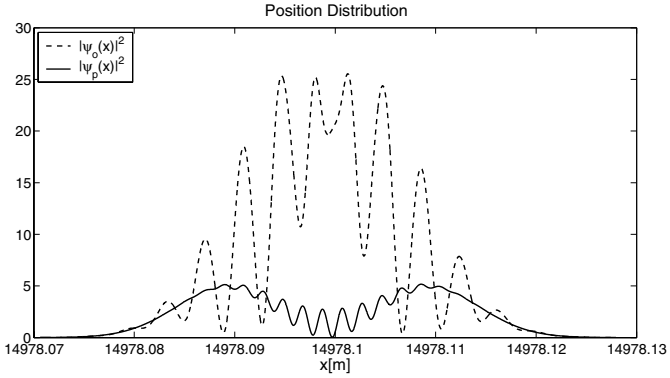

Fig. 7. With CD: $\kappa = -0.3072$ nm for $\lambda_0 = 1550$ nm, $l_g = 10$ km.

A better but still not sufficient situation may be achieved if the length l_g of the fiber is shortened to 10 km and the interferometers are unchanged, as can be seen in Figure 7. $|\psi_p(x)|^2$ exhibits 2 peaks (separated by 2 cm because of the phase shifters) which are broadened, and an interfering part is visible in between, where the pulses overlap each other including amplitude modulations. $|\psi_o(x)|^2$ is a highly oscillating function and no distinct separation is possible between the central peak and the side wings, whereas in Figure 3 this separation is clearly visible.

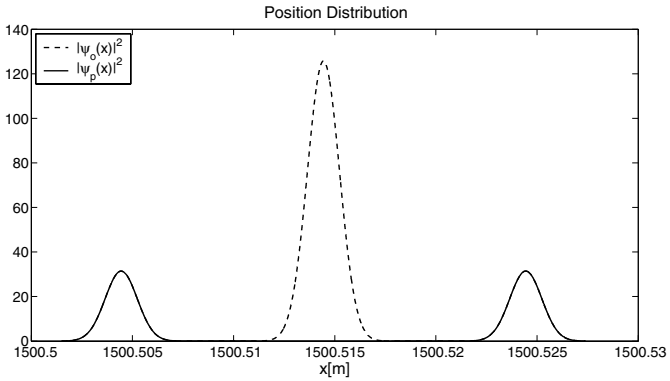

Fig. 8. With CD: $\kappa = -0.3072$ nm for $\lambda_0 = 1550$ nm, $l_g = 1$ km.

In Figure 8 $l_g = 1$ km is taken. The peaks now can be isolated as before. Left and right peaks are separated by a value of 2 cm, of course. The mean position of the left peak, for example, can be calculated using (7), (21) and (24). We obtain: $x_l = (l_g + l_c + l_n)[N_0 + 2\kappa k_0] = 1503\,\text{m} - 2.4955\,\text{m} = 1500.5045$ m as can be observed from Figure 8. CD causes a shift of -2.4955 m if $l_g = 1$ km is taken. Clearly one recognizes that the peaks have been broadened due to CD in comparison to Figure 3. One obtains from (24) and (21)

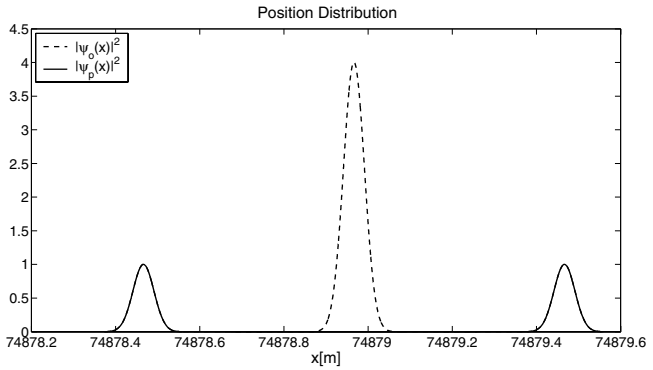

Fig. 9. With CD: the same parameters as in Figure 6 (l_g = 50 km), but with the exception that the two phase shifters are 50 times larger as before: $\Delta_d = \Delta_m = 0.5$ m.

for each of the three peaks ($ij = dm, dn, cm, cn$):

$$(\delta x)_{disp} = \frac{1}{2(\delta k)}\sqrt{\gamma_{ij}}, \tag{26}$$

$$\gamma_{ij} = 1 + 16(\delta k)^4 \delta_{ij}^2 = 1 + 16(\delta k)^4 \kappa^2 (l_g + l_i + l_j)^2. \tag{27}$$

$FWHM_{disp} = \sqrt{8\ln 2}\,(\delta x)_{disp} \approx 0.00187$ m.

The FWHM's of the wave packets have been augmented from 0.00145 m in Figure 3 (see Eq. (25)) to 0.00187 m in Figure 8 (Eq. (26)), whereas the heights are correspondingly reduced by approximately the same ratio. But observe that in Figure 3 (without CD) the length l_g of the fiber is 50 km whereas in Figure 8 (with CD) l_g is only 1 km. It can be concluded that, taking CD into account, one cannot securely perform phase coding unless the distance l_g between the 2 MZ interferometers is less or approximately 1 km provided that the parameters above are used ($\Delta_d = \Delta_m = 1$ cm). It should be noted that the wavelength distributions remain unchanged (Fig. 5) because the k^2- part of the argument of the cosine in (19) and (11) cancels out in this special case ($l_d = l_c = l_m = l_n = 1$ m).

Finally we present in Figure 9 a result, where the length l_g of the fiber is again 50 km as before, but the phase shifters Δ_d and Δ_m in both interferometers are 50 times larger, that is to say 0.5 m. The resulting plot in Figure 9 looks similar to Figure 8, because both, the phase shifts in the two interferometers and the length of the fiber l_g are increased by the same factor 50, but now the heights of the separated peaks are strongly reduced and the broadness of each peak is increased according to (26) ($FWHM_{disp} \approx 0.059$ m). Thus, using formulas (19), (22) and (26) can be very helpful in order to analyze the system under consideration.

Note that the calculations above were just simple examples. Observe that the wavelength distribution $|\alpha_{o,p}(\lambda)|^2$ of (19) and the position distribution $|\psi_{o,p}(x)|^2$ of (22) are functions of the mean wavelength λ_0, the mean square deviation of wavelengths $(\delta\lambda/\lambda_0)^2$, the group index N_0, the dispersion parameter κ, the lengths of the fibers l_i, the phase shifters Δ_i and the transmission coefficients T_i. Thus the presented formulas can be broadly applied to very different configurations of interferometric installations.

7 Summary and conclusion

In this paper, the impact of CD in a double MZ interferometer implementation, applied for phase-coding systems in quantum cryptography, has been investigated theoretically. The Gaussian wave packet description has been adopted. Thereby, the mean wavelength λ_0 and the mean square deviation $(\delta\lambda)^2$ of wavelengths describe the characteristics of the incoming beam. The two MZ interferometers are specified by means of beam splitters, the lengths of the fibers, phase shifters and absorbers. Formulas of position- and wavelength distributions, easily applicable in a simple computer program, have been developed, which are useful to examine in detail the influence of CD in such a system. A simple example has been applied, demonstrating the influence of CD on phase-coding in quantum cryptographic systems working with 2 fiber-optical MZ interferometers in series. Especially in very long glass fibers linking the 2 interferometers (for instance 50 km and more) CD becomes more and more an important factor and should be taken into consideration.

Concerning the application of the weak coherent pulse method as well as the entanglement-based method, we believe that the considerations above can be helpful for those dealing with quantum cryptographic devices like phase-coding systems based on interferometric methods using single-mode fiber optics.

This work was supported by the EC/IST Integrated Project SECOQC (Contract No. 506813). M.S. is grateful to T. Lorünser, N. Finger and M. Peev for discussion, help and assistance.

References

1. *The Physics of Quantum Information*, edited by D. Bouwmeester, A. Ekert, A. Zeilinger, 1st edn. (Springer-Verlag, Berlin, Heidelberg, New York, 2000)
2. N. Gisin, G. Ribordy, W. Tittel, H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002)
3. A.K. Ekert, J.G. Rarity, P.R. Tapster, G.M. Palma, Phys. Rev. Lett. **69**, 1293 (1992)
4. C.H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992)
5. S. Fasel, N. Gisin, G. Ribordy, H. Zbinden, Eur. Phys. J. D **30**, 143 (2004)
6. I. Marcikic, H. de Riedmatten, W. Tittel, H. Zbinden, M. Legré, N. Gisin, Phys. Rev. Lett. **93**, 180502 (2004)
7. B.E.A. Saleh, M.C. Teich, *Fundamentals of Photonics* (John Wiley & Sons, New York, 1991)
8. W.P. Schleich, *Quantum Optics in Phase Space*, 1st edn. (Wiley-VCH Verlag GmbH, Berlin, 2001)
9. M. Suda, *Quantum Interferometry in Phase Space*, 1st edn. (Springer-Verlag, Berlin, Heidelberg, New York, 2006)