PH585
Alle

Lecture # 26

Intro to quantum information processing

(Fox Ch. 12-14)

- quantum cryptography
  - use QM for secure information transfer (and detection of eavesdropper)
  - most advanced towards "real-world" applications
- quantum computing
  - use QM to enhance comput. power
- quantum teleportation
  - use QM to transfer the quantum state of one particle to another

quantum optics

- ability to generate single photons

Define: $\Phi_p = \frac{P}{\hbar\omega}$ ($\frac{\text{photons}}{s}$)

Φ_p: photon flux; P: power

Ex. Photon energy 2 eV, average power (HeNe laser, 633 nm) $P = 1\,nW$

$$\varphi = \frac{10^{-9}}{2 \times (1.6 \cdot 10^{-19})} = 3.1 \cdot 10^{9} \frac{\text{photons}}{s}$$

on average

Count photons for $\underbrace{1\,ns}_{\Delta t} \Rightarrow c\Delta t = 3 \cdot 10^{8} \frac{m}{s} \cdot 10^{-9}\,s =$

$= 0.3\,m = 30\,cm$

30 cm → 1 nW

photons = $\underbrace{3.1}_{\varphi \Delta t}$ ← "on average" (can't be fractional, but what is it really?)

⇓

Due to statistical fluctuations, due to discrete nature of photons

Instead of regularly timed stream of photons have Poisson photon statistics (for perfectly coherent light)

↑ in a beam with constant intensity

(Fox ch. 5)

$E(x,t) = E_0 \sin(kx - \omega t + \varphi)$

↑ single-mode laser

E_0, φ are time-independent

Average # photons:

$$\bar{n} = \varphi \underbrace{\frac{L}{c}}_{\Delta t}$$

Poisson distribution ⇒

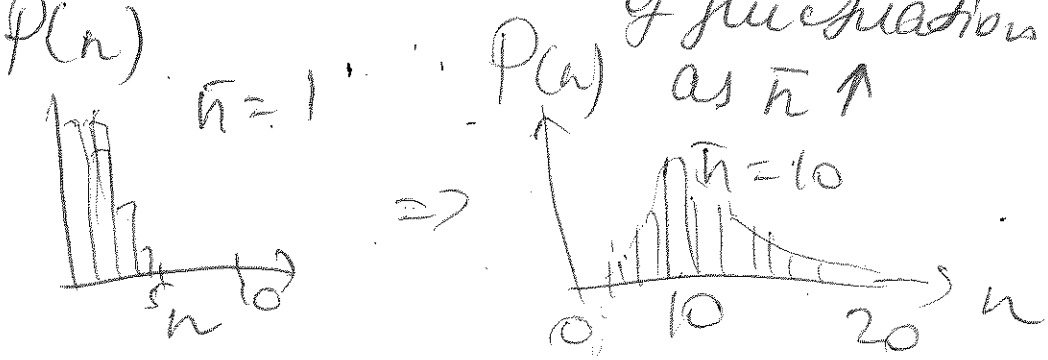
$$P(n) = \frac{\bar{n}^n}{n!} e^{-\bar{n}}, \quad n = 0, 1, 2 \ldots$$

variance = square of the standard deviation Δn

$$\text{Var}(n) = (\Delta n)^2 = \sum_{n=0}^{\infty} (n - \bar{n})^2 P(n) = \bar{n}$$

↑ for Poisson statistics

$\Delta n = \sqrt{\bar{n}}$ ⇒ relative size of fluctuation ↑ as $\bar{n}$ ↑



Other types of light: sub-Poissonian $\Delta n < \sqrt{\bar{n}}$
super-Poissonian $\Delta n > \sqrt{\bar{n}}$

Ex. An 800-nm laser pulsed at 4 MHz is attenuated to 0.1 pW.
What is: (a) $\bar{n}$ ← average # photons per pulse
(b) the fraction of pulses that have no photons
one photon, more than one photon?

(4)

(a) $\bar{n} = \eta \underbrace{\tau}_{\text{1 take}} = \frac{10^{-13}\,W}{2,5\cdot 10^{-19}\,J} \cdot \frac{1}{4\cdot 10^{6}\,s^{-1}} =$

$= 0,1$

(b) $P(0) = \frac{0,1^{0}}{0!} e^{-0,1} = 0,9048$

$n = 0$ photons

$P(1) = \frac{0,1^{1}}{1!} e^{-0,1} = 0,0905$

$P(n \geq 2) = 1 - (0,9048 + 0,0905) =$

$= 0,0047$

$\frac{P(n \geq 2)}{P(1)} = \frac{0,0047}{0,0905} = 5,2\%$

↑ Too large for a single-photon source to be used in, e.g., cryptography

develop truly single-photon sources ⇐ single molecules, QDs, point defects in semiconductors/insulators (NV centers)

From Fox "Quantum Optics"

we can see that

$$\lim_{N\to\infty}\left[\ln\left(\frac{N!}{(N-n)!N^n}\right)\right]=0.$$

Hence:

$$\lim_{N\to\infty}\left[\frac{N!}{(N-n)!N^n}\right]=1. \tag{5.10}$$

Furthermore, by applying the binomial theorem and comparing the result for the limit $N\to\infty$ to the series expansion of $\exp(-\overline{n})$, we can see that:

$$\begin{aligned}\left(1-\frac{\overline{n}}{N}\right)^{N-n} &= 1-(N-n)\frac{\overline{n}}{N}+\frac{1}{2!}(N-n)(N-n-1)\left(\frac{\overline{n}}{N}\right)^2-\cdots\\ &\to 1-\overline{n}+\frac{\overline{n}^2}{2!}-\cdots\\ &= \exp(-\overline{n}).\end{aligned} \tag{5.11}$$

On using these two limits in eqn 5.8, we find

$$\lim_{N\to\infty}[\mathcal{P}(n)]=\frac{1}{n!}\cdot 1\cdot\overline{n}^n\cdot\exp(-\overline{n}). \tag{5.12}$$

We thus conclude that the photon statistics for a coherent light wave with constant intensity are given by:

$$\mathcal{P}(n)=\frac{\overline{n}^n}{n!}e^{-\overline{n}},\quad n=0,\ 1,\ 2,\ \cdots. \tag{5.13}$$

This equation describes a **Poisson distribution.**

A summary of the mathematical properties of Poisson distributions may be found in Appendix A.

Poissonian statistics generally apply to random processes that can only return integer values. We have already mentioned one of the standard examples of Poissonian statistics, namely the number of counts from a Geiger tube pointing at a radioactive source. In this case, the number of counts is always an integer, and the average count value $\overline{n}$ is determined by the half life of the source, the amount of material present, and the time interval set by the user. The actual count values fluctuate above and below the mean value due to the random nature of the radioactive decay, and the probability for registering n counts is given by the Poissonian formula in eqn 5.13. A similar situation applies to the count rate of a photon-counting system detecting individual photons from a light beam with constant intensity. In this second case, the randomness originates from chopping the continuous beam into discrete energy packets with an equal probability of finding the energy packet within any given time subinterval.

Poisson distributions are uniquely characterized by their mean value $\overline{n}$. Representative distributions for $\overline{n}=0.1$, 1, 5, and 10 are shown in Fig. 5.3. It is apparent that the distribution peaks at $\overline{n}$ and gets broader as $\overline{n}$ increases. The fluctuations of a statistical distribution about its mean value are usually quantified in terms of the **variance**. The variance is equal to the square of the **standard deviation** Δn and is defined by:

$$\mathrm{Var}(n)\equiv(\Delta n)^2=\sum_{n=0}^{\infty}(n-\overline{n})^2\mathcal{P}(n). \tag{5.14}$$

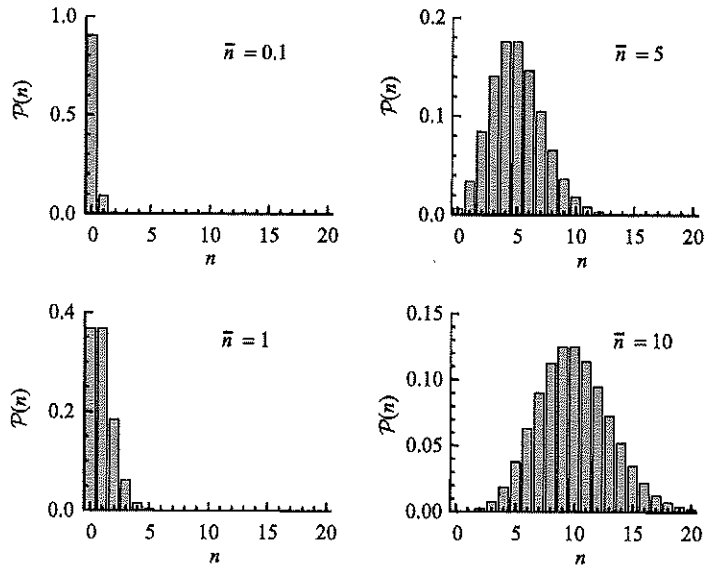


Fig. 5.3 Poisson distributions for mean values of 0.1, 1, 5, and 10. Note that the vertical axis scale changes between each figure.

It is a well-known result for Poisson statistics that the variance is equal to the mean value $\overline{n}$ (see eqn A.10):

$$(\Delta n)^2 = \overline{n}. \tag{5.15}$$

The standard deviation for the fluctuations of the photon number above and below the mean value is therefore given by:

$$\Delta n = \sqrt{\overline{n}}. \tag{5.16}$$

This shows that the relative size of the fluctuations decreases as $\overline{n}$ gets larger. If $\overline{n} = 1$, we have $\Delta n = 1$ so that $\Delta n/\overline{n} = 1$. On the other hand, if $\overline{n} = 100$, we have $\Delta n = 10$, and $\Delta n/\overline{n} = 0.1$.

Example 5.1 An attenuated beam from an argon laser operating at 514 nm (2.41 eV) with a power of 0.1 pW is detected with a photon-counting system of quantum efficiency 20% with the time interval set at 0.1 s. Calculate (a) the mean count value, and (b) the standard deviation in the count number.

Solution

(a) We first calculate the photon flux from eqn 5.1. This gives

$$\Phi = \frac{10^{-13}\ \text{W}}{2.41\ \text{eV}} = 2.59 \times 10^5\ \text{photon s}^{-1}.$$

The average photon count is then given by eqn 5.2:

$$N = 0.2 \times (2.59 \times 10^5) \times 0.1 = 5180.$$

(b) We assume that the detected counts have Poissonian statistics with a standard deviation given by eqn 5.16. With $\overline{n} \equiv N = 5180$, we then find:

$$\Delta n = \sqrt{5180} = 72.$$

process. This is a consequence of the invasive nature of quantum measurements. The eavesdroppers must reveal their presence though the disturbance they make through their measurements, which affects the results of subsequent measurements on the photons that are received at the final destination. It could be argued that the eavesdropping scheme we have considered here is very simple and that Eve might devise a more sophisticated way to tap in to the data stream. However, no matter how hard she tries, she will always be subject to the general principles and must give away something in making the measurement. We shall see how this works in practice in the next section.

12.3 Quantum key distribution according to the BB84 protocol

In the previous section we explained the general point that eavesdroppers must reveal their presence through the invasive nature of the measurements they make. We shall now see how this principle is used in practical implementations of quantum cryptography. The idea is to distribute the private key in a secure way so that Alice and Bob can subsequently use it to encrypt secret messages transmitted over public channels. There have been several schemes proposed in the literature and implemented in the laboratory, the two most important of which are:

- the Bennett–Brassard 84 (BB84) protocol,
- the Bennett 92 (B92) protocol.

In what follows we restrict our attention to the BB84 protocol, which will be sufficient to explain the basic principles. The B92 protocol is explored in Exercise 12.3.

In the simplest version of the BB84 protocol, the data are encoded as the polarization states of single photons, with binary '1' and '0' represented by orthogonal polarization states. Thus we could represent 1 by the $\theta = 0$ vertical polarization state and 0 by the $\theta = 90°$ horizontal polarization state, where the polarization angle θ is defined in Fig. 12.2. However, we are not restricted to choosing the axes of the polarization states to be horizontal or vertical. Any orthogonal pair of angles will do. In the BB84 protocol two sets of polarization states called the $\oplus$ and $\otimes$ bases are used:

The $\oplus$ basis: Binary 1 and 0 corresponds to photons with polarization angles of 0° and 90°, respectively.

The $\otimes$ basis: Binary 1 and 0 corresponds to photons with polarization angles of 45° and 135°, respectively.

The two polarization states for the $\oplus$ basis can be represented in Dirac notation by $|\updownarrow\rangle$, $|\leftrightarrow\rangle$, while the two states for the $\otimes$ basis are represented by $|\nearrow\rangle$, and $|\nwarrow\rangle$ respectively. These assignments are summarized in Table 12.1.

Table 12.1 Data representation values in the BB84 protocol for the two choices of polarization basis. θ is the polarization angle as defined in Fig. 12.2.

Basis	Binary 1	Binary 0
$\oplus$	$\|\updownarrow\rangle$ $\theta = 0°$	$\|\leftrightarrow\rangle$ $\theta = 90°$
$\otimes$	$\|\nearrow\rangle$ $\theta = 45°$	$\|\nwarrow\rangle$ $\theta = 135°$

See C. H. Bennett and G. Brassard in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, December 1984*, IEEE, New York (1984), p 175, and C. H. Bennett, *Phys. Rev. Lett.* **68**, 3121 (1992).

The orthogonal polarization states form the foundation for considering the photon as a quantum bit (qubit). See Section 13.2.

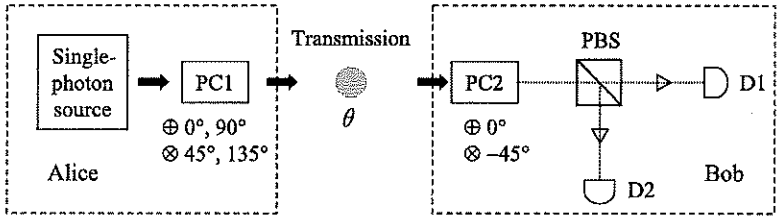


Fig. 12.4 Data encoding scheme according to the BB84 protocol. Alice has a source of vertically polarized photons and a Pockels cell PC1. PC1 rotates the polarization vector by angles of 0°, 45°, 90°, or 135° for each photon at Alice's choice. The photon that has passed through PC1 is then transmitted to Bob who detects it by using a PBS and two single-photon detectors D1 and D2 similar to the arrangement shown in Fig. 12.2. Bob's apparatus includes a second Pockels cell PC2 which can rotate the polarization vector of the incoming photon by an angle of either 0° or −45° at Bob's choice.

A Pockels cell is an electro-optic device which rotates the polarization vector of the light passing through it in proportion to the applied voltage. Many recent implementations of the BB84 protocol do not use Pockels cells any more. See Exercises 12.4 and 12.5.

An experimental scheme for quantum cryptography according to the BB84 protocol is shown in Fig. 12.4. Alice's apparatus consists of a source of vertically polarized photons and a Pockels cell PC1. Alice synchronizes her Pockels cell with the single-photon source and applies the correct voltages to produce polarization rotations of 0°, 45°, 90°, or 135°. In this way she can send a string of binary data which is encoded in either of the two polarization bases at her choice.

The photons emerging from Alice's apparatus are received by Bob who has a polarization measurement arrangement similar to the one shown in Fig. 12.2. Bob's apparatus includes a second Pockels cell PC2 in front of the PBS. Bob applies the correct voltage to this Pockels cell to rotate the polarization vector of the incoming photon by either 0° or −45° at his choice. These two choices are equivalent to detecting in the ⊕ and ⊗ bases, respectively.

Bob does not know the basis that Alice has chosen to encode the individual photons. He therefore has to choose the detection basis at random. If he guesses the right basis, he will register the correct result. This occurs when Alice chooses the ⊕ basis and Bob chooses the 0° detection angle, and also when Alice chooses the ⊗ basis and Bob chooses the −45° rotation angle. If Alice's choice of basis is random, this correct matching of bases will occur 50% of the time. For the remaining 50% of the time Bob will be detecting in the wrong basis and will get random results. Thus, for example, if the incoming photon is polarized at +45° and Bob is detecting in the ⊕ basis (rotation angle = 0°), he will register results on either of his detectors with an equal probability of 50%. (cf. eqn 12.2.)

In the BB84 protocol the following steps are taken.

1. Alice encodes her sequence of data bits according to the scheme in Table 12.1, switching randomly between the ⊕ and ⊗ bases without telling anyone what she is doing. She then transmits the photons to Bob with regular time intervals between them.

2. Bob receives the photons and records the results using a random choice of $\oplus$ and $\otimes$ detection bases as determined by the rotation angle of his Pockels cell.
3. Bob communicates with Alice over a public channel (e.g. a telephone line) and tells her his choice of detection bases, without revealing his results.
4. Alice checks Bob's choices against her own and identifies the subset of bits where both she and Bob have chosen the same basis. She tells Bob over the public channel which of the time intervals have the same choice of basis, and both Alice and Bob discard the other bits. This leaves them both with a set of sifted data bits.
5. Bob transmits to Alice over a public channel a subset of his sifted bits. Alice checks these against her own and performs an error analysis on them.
6. If the error rate is less than 25%, Alice deduces that no eavesdropping has occurred and that the quantum communication has been secure. Alice and Bob are then able to retain the remaining bits as their private key.

Table 12.2 shows an example of how these six steps of the protocol are implemented. The first line shows the original set of the data that Alice wishes to send to Bob. The second line shows the random choice of polarization basis that she makes, which gives rise to the polarization angle encoding of the photons shown in the third line using the criteria given in Table 12.1. The fourth line gives Bob's random choice of detection basis. This will coincide with Alice's for half of the bits on average. In these cases Bob will register the correct result, provided no eavesdropper is present (see below). In the other half of the cases, Bob will only get the right result with a probability of 50%. This does not matter, however, because these data are never used for the key.

The next step involves the comparison of the two bases. Bob publicly announces his choice of bases without revealing his results. Alice

Table 12.2 Representative sequence of data choices according to the BB84 protocol. θ is the polarization angle according to the encoding scheme given in Table 12.1.

A's data	1	0	0	1	1	1	0	0	1	0	0	1
A's basis	$\oplus$	$\otimes$	$\oplus$	$\otimes$	$\otimes$	$\oplus$	$\oplus$	$\otimes$	$\oplus$	$\otimes$	$\otimes$	$\oplus$
θ (°)	0	135	90	45	45	0	90	135	0	135	135	0
B's basis	$\otimes$	$\otimes$	$\oplus$	$\oplus$	$\otimes$	$\oplus$	$\otimes$	$\oplus$	$\oplus$	$\otimes$	$\oplus$	$\otimes$
B's result	1	0	0	0	1	1	0	1	1	0	1	1
Same basis ?	n	y	y	n	y	y	n	n	y	y	n	n
Sifted bits		0	0		1	1			1	0		
Data check ?		y	n		y	n			y	n		
Private key			0			1				0		

checks this against her choices and identifies the cases where the two choices coincide. These are identified with the 'y' label in the sixth row of Table 12.2. Alice tells Bob which bits these are, and they discard the other bits. This now leaves them both with the sifted bits shown in the seventh row of the table. Bob now sends a subset of his sifted bits to Alice, again over a public channel. In the example shown, he sends every other bit. Alice can check these against her own list, and carry out an error analysis.

This is the stage at which the eavesdropper reveals her presence. It is easiest to understand what happens if we assume that Eve has the same apparatus as Alice and Bob. She can then detect the photons sent by Alice using a copy of Bob's apparatus, and transmit new photons to Bob using a copy of Alice's apparatus, as shown schematically in Fig. 12.5. Since she cannot know what choice of basis Alice is making, she must choose her detection basis randomly. Half the time she will guess correctly and accurately determine the polarization state of the photon. She can then send an identically polarized photon on to Bob without anyone knowing about it. For the remaining half of the bits, she will guess incorrectly, and register a result on either of her detectors with an equal probability of 50%. She will then send a photon to Bob which is polarized with her choice of detection basis, rather than Alice's. This means that Eve will alter the polarization basis angle by 45° for 50% of the bits. In the cases where Bob has chosen the same basis as Alice and Eve has guessed incorrectly, Bob will register random results on his detectors with a probability of 50%. He will thus register errors even when he has guessed Alice's basis correctly. The error probability $\mathcal{P}_{\text{error}}$ is given by:

$$\begin{aligned} \mathcal{P}_{\text{error}} &= \mathcal{P}_{\text{Eve has wrong basis}} \times \mathcal{P}_{\text{Bob gets wrong result}}, \\ &= 50\% \times 50\%, \\ &= 25\%. \end{aligned} \tag{12.3}$$

This high error rate of 25% will be easily recognizable when Alice carries out her error analysis in the final step of the process. She will thus be able to detect the presence of the eavesdropper, and therefore know whether the private key distribution has been secure.

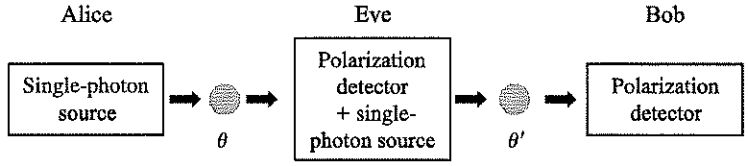


Fig. 12.5 An eavesdropper between Alice and Bob tries to measure the polarization angle θ of the photon sent by Alice and send an identical photon on to Bob. She reveals her presence because the polarization angle θ' of the second photon will be different from θ for 50% of the photons.