

Appendix S1

Solutions to Chapter 1 exercises

Solution to Exercise 1.1. Using the result of Ex. A.15, we write (don't forget the complex conjugation where appropriate!)

$$\begin{aligned}\langle \psi | \psi \rangle &= N^2(2 \langle \text{alive} | \psi \rangle - i \langle \text{dead} | \psi \rangle) \\ &= N^2(4 \langle \text{alive} | \text{alive} \rangle + 2i \langle \text{alive} | \text{dead} \rangle) - 2i \langle \text{dead} | \text{alive} \rangle + \langle \text{dead} | \text{dead} \rangle.\end{aligned}\quad (\text{S1.1})$$

Now since $|\text{dead}\rangle$ and $|\text{alive}\rangle$ are physical states, their norms equal 1. On the other hand, these states are incompatible with each other, so their inner product vanishes. Hence we have $\langle \psi | \psi \rangle = N^2(4 + 1) = 5N^2$ and hence $N = 1/\sqrt{5}$.

Solution to Exercise 1.2. Although the motion is one-dimensional, all position states are incompatible with each other: $\langle x | x' \rangle = 0$ unless $x = x'$. Therefore there are infinitely many linearly independent states, and the dimension of the Hilbert space is infinite.

Solution to Exercise 1.3. There are two vectors in each set. Because our Hilbert space is two-dimensional, and according to Ex. A.19, it is enough to show that each set is orthonormal in order for it to be a basis. We calculate the inner products by expressing the vectors in the matrix form, in the canonical basis according to Table 1.1.

a) For the diagonal states, we find

$$\begin{aligned}\langle + | + \rangle &= \frac{1}{2} (1 \ 1) \begin{pmatrix} 1 \\ 1 \end{pmatrix} = 1; \\ \langle - | + \rangle &= \frac{1}{2} (1 \ -1) \begin{pmatrix} 1 \\ 1 \end{pmatrix} = 0; \\ \langle + | - \rangle &= \frac{1}{2} (1 \ 1) \begin{pmatrix} 1 \\ -1 \end{pmatrix} = 0; \\ \langle - | - \rangle &= \frac{1}{2} (1 \ -1) \begin{pmatrix} 1 \\ -1 \end{pmatrix} = 1.\end{aligned}$$

b) Similarly, for the circular states [we perform complex conjugation according to Eq. (A.5)]:

$$\begin{aligned}\langle R|R\rangle &= \frac{1}{2}(1-i)\begin{pmatrix} 1 \\ i \end{pmatrix} = 1; \\ \langle L|R\rangle &= \frac{1}{2}(1+i)\begin{pmatrix} 1 \\ i \end{pmatrix} = 0; \\ \langle R|L\rangle &= \frac{1}{2}(1-i)\begin{pmatrix} 1 \\ -i \end{pmatrix} = 0; \\ \langle L|L\rangle &= \frac{1}{2}(1+i)\begin{pmatrix} 1 \\ -i \end{pmatrix} = 1.\end{aligned}$$

Solution to Exercise 1.4. For the diagonal basis, we find, using Table 1.1:

$$\begin{aligned}\langle +|H\rangle &= \frac{1}{\sqrt{2}}(1\ 1)\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}}; \\ \langle -|H\rangle &= \frac{1}{\sqrt{2}}(1\ -1)\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}}; \\ \langle +|V\rangle &= \frac{1}{\sqrt{2}}(1\ 1)\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}}; \\ \langle -|V\rangle &= \frac{1}{\sqrt{2}}(1\ -1)\begin{pmatrix} 0 \\ 1 \end{pmatrix} = -\frac{1}{\sqrt{2}},\end{aligned}$$

and thus $|H\rangle = (|+\rangle + |-\rangle)/\sqrt{2}$; $|V\rangle = (|+\rangle - |-\rangle)/\sqrt{2}$. Similarly for the circular polarization basis,

$$\begin{aligned}\langle R|H\rangle &= \frac{1}{\sqrt{2}}(1-i)\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}}; \\ \langle L|H\rangle &= \frac{1}{\sqrt{2}}(1+i)\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}}; \\ \langle R|V\rangle &= \frac{1}{\sqrt{2}}(1-i)\begin{pmatrix} 0 \\ 1 \end{pmatrix} = -\frac{i}{\sqrt{2}}; \\ \langle L|V\rangle &= \frac{1}{\sqrt{2}}(1+i)\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \frac{i}{\sqrt{2}},\end{aligned}$$

hence $|H\rangle = (|R\rangle + |L\rangle)/\sqrt{2}$; $|V\rangle = i(-|R\rangle + |L\rangle)/\sqrt{2}$.

Solution to Exercise 1.5. Using Table 1.1, we express states $|a\rangle$ and $|b\rangle$ in the canonical basis:

$$\begin{aligned}|a\rangle &= |30^\circ\rangle = \frac{\sqrt{3}|H\rangle + |V\rangle}{2} \simeq \frac{1}{2}\begin{pmatrix} \sqrt{3} \\ 1 \end{pmatrix} \\ |b\rangle &= |-30^\circ\rangle = \frac{\sqrt{3}|H\rangle - |V\rangle}{2} \simeq \frac{1}{2}\begin{pmatrix} \sqrt{3} \\ -1 \end{pmatrix}.\end{aligned}$$

We now follow the same approach as in the previous exercise.

$$\langle +|a \rangle \stackrel{\text{canonical basis}}{\simeq} \frac{1}{2\sqrt{2}} (1 \ 1) \begin{pmatrix} \sqrt{3} \\ 1 \end{pmatrix} = \frac{\sqrt{3}+1}{2\sqrt{2}};$$

$$\langle -|a \rangle \stackrel{\text{canonical basis}}{\simeq} \frac{1}{2\sqrt{2}} (1 \ -1) \begin{pmatrix} \sqrt{3} \\ 1 \end{pmatrix} = \frac{\sqrt{3}-1}{2\sqrt{2}}$$

and thus, the decomposition of $|a\rangle$ in the diagonal polarization basis is,

$$|a\rangle \stackrel{\text{diagonal basis}}{\simeq} \begin{pmatrix} \langle +|a \rangle \\ \langle -|a \rangle \end{pmatrix} = \frac{1}{2\sqrt{2}} \begin{pmatrix} \sqrt{3}+1 \\ \sqrt{3}-1 \end{pmatrix}. \quad (\text{S1.2})$$

Similarly, we obtain

$$|b\rangle \stackrel{\text{diagonal basis}}{\simeq} \frac{1}{2\sqrt{2}} \begin{pmatrix} \sqrt{3}-1 \\ \sqrt{3}+1 \end{pmatrix}. \quad (\text{S1.3})$$

For the circular polarization basis,

$$\langle R|a \rangle \stackrel{\text{canonical basis}}{\simeq} \frac{1}{2\sqrt{2}} (1 \ -i) \begin{pmatrix} \sqrt{3} \\ 1 \end{pmatrix} = \frac{\sqrt{3}-i}{2\sqrt{2}};$$

$$\langle L|a \rangle \stackrel{\text{canonical basis}}{\simeq} \frac{1}{2\sqrt{2}} (1 \ i) \begin{pmatrix} \sqrt{3} \\ 1 \end{pmatrix} = \frac{\sqrt{3}+i}{2\sqrt{2}}$$

therefore

$$|a\rangle \stackrel{\text{circular basis}}{\simeq} \frac{1}{2\sqrt{2}} \begin{pmatrix} \sqrt{3}-i \\ \sqrt{3}+i \end{pmatrix} \quad (\text{S1.4})$$

and similarly

$$|b\rangle \stackrel{\text{circular basis}}{\simeq} \frac{1}{2\sqrt{2}} \begin{pmatrix} \sqrt{3}+i \\ \sqrt{3}-i \end{pmatrix}. \quad (\text{S1.5})$$

To find the inner product in each of the three bases, we use Eq. (A.5).

$$\langle a|b \rangle_{\text{canonical basis}} \simeq \frac{1}{4} (\sqrt{3} \ 1) \begin{pmatrix} \sqrt{3} \\ -1 \end{pmatrix} = \frac{1}{2}$$

$$\langle a|b \rangle_{\text{diagonal basis}} \simeq \frac{1}{8} (\sqrt{3}+1 \ \sqrt{3}-1) \begin{pmatrix} \sqrt{3}-1 \\ \sqrt{3}+1 \end{pmatrix} = \frac{1}{2}$$

$$\langle a|b \rangle_{\text{circular basis}} \simeq \frac{1}{8} (\sqrt{3}+i \ \sqrt{3}-i) \begin{pmatrix} \sqrt{3}+i \\ \sqrt{3}-i \end{pmatrix} = \frac{1}{2}$$

and all three inner products are the same, confirming the theory.

Solution to Exercise 1.6. According to Eq. (A.7), state $|\psi\rangle$ decomposes into basis $|v_i\rangle$ according to

$$|\psi\rangle = \sum_i \langle v_i | \psi \rangle |v_i\rangle. \quad (\text{S1.6})$$

Hence,

$$\langle \psi | \psi \rangle = \sum_{i,j} \langle v_j | \psi \rangle^* \langle v_i | \psi \rangle \langle v_j | v_i \rangle \quad (\text{S1.7})$$

$$= \sum_{i,j} \langle v_j | \psi \rangle^* \langle v_i | \psi \rangle \delta_{ij} \quad (\text{S1.8})$$

$$= \sum_i |\langle v_i | \psi \rangle|^2 \quad (\text{S1.9})$$

$$\stackrel{(1.3)}{=} \sum_i \text{pr}_i. \quad (\text{S1.10})$$

Solution to Exercise 1.7. Suppose state $|\psi\rangle$, measured in basis $\{|v_i\rangle\}$, gives probabilities $\text{pr}_i = |\langle v_i | \psi \rangle|^2$. Then for state $|\psi'\rangle = e^{i\phi} |\psi\rangle$, we have

$$\text{pr}'_i = |e^{i\phi} \langle v_i | \psi \rangle|^2 = |e^{i\phi}|^2 |\langle v_i | \psi \rangle|^2 = |\langle v_i | \psi \rangle|^2 = \text{pr}_i.$$

Solution to Exercise 1.8.

- As we found in Ex. C.8, state $|45^\circ\rangle$ after propagating through a waveplate at 22.5° will become $|H\rangle$ and subsequently be transmitted through the PBS. State $|-45^\circ\rangle$, on the other hand, will become $|V\rangle$ and reflect from the PBS. Hence these two states will generate “clicks” in two different photon detectors and can therefore be distinguished by this apparatus.
- As found in Ex. C.9, the two circularly polarized states, propagating through a quarter-waveplate at 0° , will transform into the diagonally polarized states. The subsequent part of the apparatus is equivalent to that of part (a), and hence can distinguish between these states.

Solution to Exercise 1.10. The apparatus would be similar to that in Fig. 1.2(b), but the waveplate’s optic axis would need to be at the angle $\theta/2$ to horizontal. Such a waveplate will convert state $|\theta\rangle$ into $|H\rangle$ and $|\frac{\pi}{2} + \theta\rangle$ into $|V\rangle$.

Solution to Exercise 1.11. One $\lambda/4$ waveplate with its optic axis oriented at 45° from horizontal would do the trick. In the reference frame of that waveplate, states $|H\rangle$ and $|V\rangle$ appear diagonally polarized, so the waveplate would interconvert states between the canonical and circular bases according to $|H\rangle \rightarrow |R\rangle \rightarrow |V\rangle \rightarrow |L\rangle \rightarrow |H\rangle$. Hence such a waveplate, followed by a polarizing beam splitter, will send all right circularly polarized photons to one detector and left to another.

Solution to Exercise 1.12.

- We use the theorem of total probability (Ex. B.6). Given that the input is either $|H\rangle$ with probability $1/2$ or $|V\rangle$ with probability $1/2$, and using the result of Ex. 1.9, we find

$$\begin{aligned}\text{pr}_H &= \frac{1}{2}\text{pr}_{H|H} + \frac{1}{2}\text{pr}_{H|V} = \frac{1}{2}; \\ \text{pr}_V &= \frac{1}{2}\text{pr}_{V|H} + \frac{1}{2}\text{pr}_{V|V} = \frac{1}{2}.\end{aligned}$$

b) Similarly,

$$\begin{aligned}\text{pr}_+ &= \frac{1}{2}\text{pr}_{+|H} + \frac{1}{2}\text{pr}_{+|V} = \frac{1}{2}; \\ \text{pr}_- &= \frac{1}{2}\text{pr}_{-|H} + \frac{1}{2}\text{pr}_{-|V} = \frac{1}{2}.\end{aligned}$$

c) Similarly,

$$\begin{aligned}\text{pr}_R &= \frac{1}{2}\text{pr}_{R|H} + \frac{1}{2}\text{pr}_{R|V} = \frac{1}{2}; \\ \text{pr}_L &= \frac{1}{2}\text{pr}_{L|H} + \frac{1}{2}\text{pr}_{L|V} = \frac{1}{2}.\end{aligned}$$

Solution to Exercise 1.13. We use the decompositions found in Ex. 1.5.

a)

$$\begin{aligned}\text{pr}_H &= |\langle 30^\circ | H \rangle|^2 = \left| \frac{1}{2} (\sqrt{3} \ 1) \begin{pmatrix} 1 \\ 0 \end{pmatrix} \right|^2 = \left| \frac{\sqrt{3}}{2} \right|^2 = \frac{3}{4} \\ \text{pr}_V &= |\langle 30^\circ | V \rangle|^2 = \left| \frac{1}{2} (\sqrt{3} \ 1) \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right|^2 = \left| \frac{1}{2} \right|^2 = \frac{1}{4}\end{aligned}$$

Hence the measurement gives a 75% chance of being in state $|H\rangle$ and a 25% chance of being in state $|V\rangle$.

b)

$$\begin{aligned}\text{pr}_+ &= |\langle 30^\circ | + \rangle|^2 = \left| \frac{1}{2\sqrt{2}} (\sqrt{3} \ 1) \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right|^2 = \left| \frac{\sqrt{3}+1}{2\sqrt{2}} \right|^2 = \frac{4+2\sqrt{3}}{8} = 0.933 \\ \text{pr}_- &= |\langle 30^\circ | - \rangle|^2 = \left| \frac{1}{2\sqrt{2}} (\sqrt{3} \ 1) \begin{pmatrix} 1 \\ -1 \end{pmatrix} \right|^2 = \left| \frac{\sqrt{3}-1}{2\sqrt{2}} \right|^2 = \frac{4-2\sqrt{3}}{8} = 0.067\end{aligned}$$

c)

$$\begin{aligned}\text{pr}_R &= |\langle 30^\circ | R \rangle|^2 = \left| \frac{1}{2\sqrt{2}} (\sqrt{3} \ 1) \begin{pmatrix} 1 \\ i \end{pmatrix} \right|^2 = \left| \frac{\sqrt{3}-i}{2\sqrt{2}} \right|^2 = \frac{1}{2} \\ \text{pr}_L &= |\langle 30^\circ | L \rangle|^2 = \left| \frac{1}{2\sqrt{2}} (\sqrt{3} \ 1) \begin{pmatrix} 1 \\ -i \end{pmatrix} \right|^2 = \left| \frac{\sqrt{3}+i}{2\sqrt{2}} \right|^2 = \frac{1}{2}\end{aligned}$$

Solution to Exercise 1.14.

$$\text{pr}_+ = |\langle + | \psi \rangle|^2 \quad (\text{S1.11a})$$

$$\begin{aligned} &= \left| \left(\frac{\langle H | + \langle V |}{\sqrt{2}} \right) \left(\frac{|H\rangle + e^{i\phi} |V\rangle}{\sqrt{2}} \right) \right|^2 \\ &= \frac{1}{4} |\langle H | H \rangle + e^{i\phi} \langle H | V \rangle + \langle V | H \rangle + e^{i\phi} \langle V | V \rangle|^2 \\ &= \frac{1}{4} |1 + 0 + 0 + e^{i\phi}|^2 \\ &= \frac{1}{2} (1 + \cos \phi); \end{aligned}$$

$$\text{pr}_- = |\langle - | \psi \rangle|^2 \quad (\text{S1.11b})$$

$$\begin{aligned} &= \left| \left(\frac{\langle H | - \langle V |}{\sqrt{2}} \right) \left(\frac{|H\rangle + e^{i\phi} |V\rangle}{\sqrt{2}} \right) \right|^2 \\ &= \frac{1}{4} |\langle H | H \rangle + e^{i\phi} \langle H | V \rangle - \langle V | H \rangle - e^{i\phi} \langle V | V \rangle|^2 \\ &= \frac{1}{4} |1 + 0 - 0 - e^{i\phi}|^2 \\ &= \frac{1}{2} (1 - \cos \phi). \end{aligned}$$

As expected, $\text{pr}_+ + \text{pr}_- = 1$.

Solution to Exercise 1.15. For a general polarization state $|\psi\rangle = \psi_H |H\rangle + \psi_V |V\rangle$, let us express $\psi_H = a_H e^{i\phi_H}$ and $\psi_V = a_V e^{i\phi_V}$, where the ϕ 's are real, a 's are both real and non-negative. Recalling that a change in the overall phase of the system does not affect its physics, we may multiply the state $|\psi\rangle$ by the phase factor $e^{-i\phi_V}$, so that $|\psi\rangle = r_H |H\rangle + r_V e^{i\phi} |V\rangle$ (where we have defined the new variable $\phi \equiv \phi_V - \phi_H$). Our task is to find three unknown variables, r_H , r_V and ϕ .

We first look at the measurement in the canonical basis. The probability to detect a horizontally polarized photon is

$$\text{pr}_H = |\langle H | \psi \rangle|^2 = \left| (1 \ 0) \begin{pmatrix} r_H \\ r_V e^{i\phi} \end{pmatrix} \right|^2 = r_H^2,$$

from which we find

$$\begin{aligned} r_H &= \sqrt{\text{pr}_H} \\ r_V &= \sqrt{1 - r_H^2} = \sqrt{1 - \text{pr}_H}. \end{aligned}$$

Here we used the facts that both r_H and r_V are real and positive, as well as the normalization condition $\langle \psi | \psi \rangle = r_H^2 + |r_V e^{i\phi}|^2 = r_H^2 + r_V^2 = 1$.

It remains to determine ϕ . We write the probability of detecting the $+45^\circ$ polarized state as follows:

$$\begin{aligned}
\text{pr}_+ &= |\langle + | \psi \rangle|^2 = \left| \frac{1}{\sqrt{2}} (1 \ 1) \begin{pmatrix} r_H \\ r_V e^{i\phi} \end{pmatrix} \right|^2 \\
&= 1/2 |r_H + r_V e^{i\phi}|^2 \\
&= 1/2 [r_H^2 + r_V^2 + r_H r_V (e^{i\phi} + e^{-i\phi})] \\
&= 1/2 + r_H r_V \cos \phi
\end{aligned}$$

and for the right circularly polarized state

$$\begin{aligned}
\text{pr}_R &= |\langle R | \psi \rangle|^2 = \left| \frac{1}{\sqrt{2}} (1 \ -i) \begin{pmatrix} r_H \\ r_V e^{i\phi} \end{pmatrix} \right|^2 \\
&= 1/2 |r_H - i r_V e^{i\phi}|^2 \\
&= 1/2 [r_H^2 + r_V^2 - i r_H r_V (e^{i\phi} - e^{-i\phi})] \\
&= 1/2 + r_H r_V \sin \phi.
\end{aligned}$$

Each of these equations do not identify ϕ unambiguously. For example, states $|R\rangle$ and $|L\rangle$ (for which $\phi = \pm\pi/2$, respectively) both have $\cos \phi = 0$ and hence cannot be distinguished through a canonical and diagonal basis measurements alone. However, the two equations taken together give us both the sine and cosine, allowing us to unambiguously determine the value of ϕ .

Solution to Exercise 1.16.

- Assume for simplicity that the space we want to measure states in is two-dimensional. An apparatus that is able to resolve one of the states, say $|a\rangle$, with perfect certainty, must include a projective measurement associated with the basis $\{|a\rangle, |a_\perp\rangle\}$, where $|a_\perp\rangle$ is some state that is orthogonal to $|a\rangle$. If this apparatus is now applied to perform measurement on state $|b\rangle$, it has a nonzero probability $|\langle a | b \rangle|^2$ to point onto $|a\rangle$. Therefore, with some probability, the projective measurement will yield the same outcome for $|a\rangle$ and $|b\rangle$. No matter what classical processing the output of this measurement is subjected to, this inconclusiveness will persist.
- Such a device could be made with two sub-devices, one measuring in the $\{|a\rangle, |a_\perp\rangle\}$ basis, one measuring in the $\{|b\rangle, |b_\perp\rangle\}$ basis, and a randomizer that sends states to one or the other sub-device randomly — for example, a non-polarizing beam splitter. If the second sub-device detects a $|b_\perp\rangle$ state, one would know the input state was certainly not $|b\rangle$, so it must be $|a\rangle$. Similarly, if the first sub-device detects a $|a_\perp\rangle$ state, the input state is certainly $|b\rangle$. In the event of any other outcome, the input state is uncertain.

Solution to Exercise 1.17. The photon has a 50% probability to go either into the upper or lower path. If it goes into the lower path, the bomb will detonate. If it goes into the upper path, it will leave the interferometer in the vertical polarization state and will with equal probability land on either detector “+” or “-”. The probability of the event in each detector is thus 25%. In the event of a click of detector “-”, the bomb is detected. If detector “+” clicks, the result is inconclusive.

Solution to Exercise 1.18. First, note that only those events will contribute to the error rate in which Alice and Bob use the same basis. In approximately 1/2 events, Eve will also be using this basis, then she will not introduce an error. In the remaining 1/2 events, Eve will intercept and resend a photon in a wrong basis, which will be then randomly detected by one of Bob’s detectors. With probability 1/2, it will be the “incorrect” detector, so

Bob will record a bit value that is different from that sent by Alice. Therefore the overall probability of error in the final key is $1/2 \times 1/2 = 1/4$.

Solution to Exercise 1.19. The loss will not affect the security because Alice and Bob, when generating the secret key, do not use the data from those events in which the photon has been lost.

Solution to Exercise 1.20.

- a) A loss rate of 5% per km implies that $n(L) = n_0 e^{-\beta L} = 0.95 n_0$ for $L = 1$ km. Accordingly, $\beta = -(\ln 0.95) \text{ km}^{-1} \approx 0.0513 \text{ km}^{-1}$.
- b) For $L = 300$ km, $e^{-\beta L} \approx e^{-15} \approx 2 \times 10^{-7}$.

Solution to Exercise 1.21. Out of the n_0 photons sent by Alice every second, $n_0 e^{-\beta L}$ will reach Bob; each of them will be detected with probability η . Of the detected photons, one-half will be used to generate the secret key, so the quantum bit transfer rate is¹ $\eta n_0 e^{-\beta L} / 2$. Additionally, the two Bob's detectors generate dark counts at a rate $2f_d$, but a half of that rate will correspond to events in which Alice and Bob chose different bases. Of the remaining half, only one-half of the events will be in the "wrong" detector, thereby generating an error in the secret key. So the quantum bit error rate is $f_d/2$.

The fraction of error in the produced secret key is, accordingly, $f_d / (f_d + \eta n_0 e^{-\beta L})$. When this fraction becomes higher than 11%, security is not guaranteed. This happens at $L \approx 200$ km for $n_0 = 2 \times 10^7 \text{ s}^{-1}$ and 340 km for $n_0 = 2 \times 10^{10} \text{ s}^{-1}$ (Fig. 1.5).

Solution to Exercise 1.22. Using the result of Exercise A.45, we write:

$$|+\rangle\langle-| \stackrel{\text{canonical basis}}{\simeq} \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \frac{1}{\sqrt{2}} (1 \ -1) = \frac{1}{2} \begin{pmatrix} 1 & -1 \\ 1 & -1 \end{pmatrix}.$$

Using the same approach for the $\{|R\rangle, |L\rangle\}$ basis would require obtaining the expressions for $|+\rangle$ and $|-\rangle$ in that basis. As an alternative technique, we use the expression (A.21) for converting an operator from the Dirac to matrix form:

¹ The actual secret key transfer rate is somewhat lower due to the overhead associated with the privacy amplification.

$$\begin{aligned}\langle R|(|+\rangle\langle-|)|R\rangle &= \langle R|+\rangle\langle-|R\rangle \\ &= \left[\frac{1}{\sqrt{2}}(1-i)\frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix}\right] \left[\frac{1}{\sqrt{2}}(1-1)\frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ i \end{pmatrix}\right] = \frac{-i}{2}\end{aligned}$$

$$\begin{aligned}\langle R|(|+\rangle\langle-|)|L\rangle &= \langle R|+\rangle\langle-|L\rangle \\ &= \left[\frac{1}{\sqrt{2}}(1-i)\frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix}\right] \left[\frac{1}{\sqrt{2}}(1-1)\frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -i \end{pmatrix}\right] = \frac{1}{2}\end{aligned}$$

$$\begin{aligned}\langle L|(|+\rangle\langle-|)|R\rangle &= \langle L|+\rangle\langle-|R\rangle \\ &= \left[\frac{1}{\sqrt{2}}(1+i)\frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix}\right] \left[\frac{1}{\sqrt{2}}(1-1)\frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ i \end{pmatrix}\right] = \frac{1}{2}\end{aligned}$$

$$\begin{aligned}\langle L|(|+\rangle\langle-|)|L\rangle &= \langle L|+\rangle\langle-|L\rangle \\ &= \left[\frac{1}{\sqrt{2}}(1+i)\frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix}\right] \left[\frac{1}{\sqrt{2}}(1-1)\frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -i \end{pmatrix}\right] = \frac{i}{2}\end{aligned}$$

and hence the matrix is

$$|+\rangle\langle-| \stackrel{\text{circular basis}}{\simeq} \frac{1}{2} \begin{pmatrix} -i & 1 \\ 1 & i \end{pmatrix} \quad (\text{S1.12})$$

Solution to Exercise 1.23.

a) Using Eq. (A.25), we write

$$\begin{aligned}\hat{A} &= |R\rangle\langle H| + 2|H\rangle\langle V| \\ &= \frac{1}{\sqrt{2}}(|H\rangle + i|V\rangle)\langle H| + 2|H\rangle\langle V| \\ &= \frac{1}{\sqrt{2}}|H\rangle\langle H| + \frac{i}{\sqrt{2}}|V\rangle\langle H| + 2|H\rangle\langle V|,\end{aligned}$$

which, according to Eq. (A.24), corresponds to the matrix

$$\hat{A} \simeq \begin{pmatrix} 1/\sqrt{2} & 2 \\ i/\sqrt{2} & 0 \end{pmatrix}. \quad (\text{S1.13})$$

b) Similarly,

$$\begin{aligned}\hat{A} &= |R\rangle\langle+| + |H\rangle\langle-| \\ &= \frac{1}{2}(|H\rangle + i|V\rangle)(\langle H| + \langle V|) + \frac{1}{\sqrt{2}}|H\rangle(\langle H| - \langle V|) \\ &= \left(\frac{1}{2} + \frac{1}{\sqrt{2}}\right)|H\rangle\langle H| + \left(\frac{1}{2} - \frac{1}{\sqrt{2}}\right)|H\rangle\langle V| + \frac{i}{2}|V\rangle\langle H| + \frac{i}{2}|V\rangle\langle V|,\end{aligned}$$

so we obtain the matrix

$$\hat{A} \simeq \begin{pmatrix} \frac{1}{2} + \frac{1}{\sqrt{2}} & \frac{1}{2} - \frac{1}{\sqrt{2}} \\ \frac{i}{2} & \frac{i}{2} \end{pmatrix}. \quad (\text{S1.14})$$

Solution to Exercise 1.24.

a) From Eqs. A.25 and (1.4), we obtain

$$\hat{A}_{\Delta\varphi} = e^{i\Delta\varphi} |\alpha\rangle\langle\alpha| + \left| \frac{\pi}{2} + \alpha \right\rangle \left\langle \frac{\pi}{2} + \alpha \right|. \quad (\text{S1.15})$$

b) We know from Table 1.1 that $|\alpha\rangle \simeq \begin{pmatrix} \cos\alpha \\ \sin\alpha \end{pmatrix}$ and $|\frac{\pi}{2} + \alpha\rangle \simeq \begin{pmatrix} \cos(\frac{\pi}{2} + \alpha) \\ \sin(\frac{\pi}{2} + \alpha) \end{pmatrix} = \begin{pmatrix} -\sin\alpha \\ \cos\alpha \end{pmatrix}$. Hence we can write

$$\begin{aligned} \hat{A}_{\Delta\varphi} &\simeq e^{i\Delta\varphi} \begin{pmatrix} \cos\alpha \\ \sin\alpha \end{pmatrix} \begin{pmatrix} \cos\alpha & \sin\alpha \end{pmatrix} + \begin{pmatrix} -\sin\alpha \\ \cos\alpha \end{pmatrix} \begin{pmatrix} -\sin\alpha & \cos\alpha \end{pmatrix} \\ &= \begin{pmatrix} e^{i\Delta\varphi} \cos^2\alpha + \sin^2\alpha & (e^{i\Delta\varphi} - 1) \sin\alpha \cos\alpha \\ (e^{i\Delta\varphi} - 1) \sin\alpha \cos\alpha & e^{i\Delta\varphi} \sin^2\alpha + \cos^2\alpha \end{pmatrix}. \end{aligned}$$

c) For a half-wave plate, $\Delta\varphi = \pi$ so $e^{i\Delta\varphi} = -1$. For a quarter-wave plate, $\Delta\varphi = \pi/2$ so $e^{i\Delta\varphi} = i$. Substituting this into $\hat{A}_{\Delta\varphi}$, we obtain Eq. (1.5) (for the half-wave plate, we also need to apply the trigonometric identities for the sine and cosine of a double argument).

Solution to Exercise 1.25.

a) Writing $|\theta\rangle = \begin{pmatrix} \cos\theta \\ \sin\theta \end{pmatrix}$, we find

$$\begin{aligned} \hat{A}_{\text{HWP}}(\alpha) |\theta\rangle &\stackrel{(1.5a)}{\simeq} \begin{pmatrix} -\cos 2\alpha & -\sin 2\alpha \\ -\sin 2\alpha & \cos 2\alpha \end{pmatrix} \begin{pmatrix} \cos\theta \\ \sin\theta \end{pmatrix} \\ &= \begin{pmatrix} -\cos 2\alpha \cos\theta - \sin 2\alpha \sin\theta \\ -\sin 2\alpha \cos\theta + \cos 2\alpha \sin\theta \end{pmatrix} \\ &= \begin{pmatrix} -\cos(2\alpha - \theta) \\ -\sin(2\alpha - \theta) \end{pmatrix} \\ &\simeq -|2\alpha - \theta\rangle. \end{aligned}$$

b) A quarter-wave plate with its optic axis oriented horizontally has $\alpha = 0$ so Eq. (1.5b) takes the form $\hat{A}_{\text{QWP}}(0) = \begin{pmatrix} i & 0 \\ 0 & 1 \end{pmatrix}$. Applying these to the diagonal and circular polarization states, we find

$$\begin{aligned}\hat{A}_{\text{QWP}}(0)|+\rangle &\simeq \frac{1}{\sqrt{2}} \begin{pmatrix} i & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} i \\ 1 \end{pmatrix} \simeq i|L\rangle; \\ \hat{A}_{\text{QWP}}(0)|L\rangle &\simeq \frac{1}{\sqrt{2}} \begin{pmatrix} i & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ -i \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} i \\ -i \end{pmatrix} \simeq i|-\rangle; \\ \hat{A}_{\text{QWP}}(0)|-\rangle &\simeq \frac{1}{\sqrt{2}} \begin{pmatrix} i & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ -1 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} i \\ -1 \end{pmatrix} \simeq i|R\rangle; \\ \hat{A}_{\text{QWP}}(0)|R\rangle &\simeq \frac{1}{\sqrt{2}} \begin{pmatrix} i & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ i \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} i \\ i \end{pmatrix} \simeq i|+\rangle.\end{aligned}$$

Solution to Exercise 1.26. By referring to Eq. (1.5a) we find that the the matrix representation (in the canonical basis) of a $\lambda/2$ waveplate with its optic axis oriented vertically is the $\hat{\sigma}_z$ operator. This waveplate is all that is necessary to implement the $\hat{\sigma}_z$ operator.

Similarly [Ex. 1.24(b)], a $\lambda/2$ waveplate with its optic axis oriented at a 135° degree angle from horizontal is sufficient to implement the $\hat{\sigma}_x$ operator.

If we have a sequence of optical elements being applied to the photon, the operator for this sequence can be found by multiplying the operators of the individual elements together (in the reverse order, i.e. the operator corresponding to the first optical element is placed last in the expression for the product). Because

$$\hat{\sigma}_z \hat{\sigma}_x \simeq \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = i \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \simeq i\hat{\sigma}_y,$$

the Pauli operator $\hat{\sigma}_y$ may be implemented (up to an overall phase factor) using a $\lambda/2$ waveplate with its optic axis oriented at 135° followed by a $\lambda/2$ waveplate with its optic axis oriented vertically.

Solution to Exercise 1.27.

a) Referring to Eq. (A.24), we find

$$\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \simeq \frac{1}{\sqrt{2}} (|H\rangle\langle H| + |H\rangle\langle V| + |V\rangle\langle H| - |V\rangle\langle V|). \quad (\text{S1.16})$$

b)

$$\begin{aligned}\hat{H}|H\rangle &\simeq \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \simeq |45^\circ\rangle \\ \hat{H}|V\rangle &\simeq \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} \simeq |-45^\circ\rangle\end{aligned} \quad (\text{S1.17})$$

c) Matrix (1.5a) takes the form of the Hadamard matrix for $2\alpha = 5\pi/4$. The Hadamard operation can be therefore be implemented by a $\lambda/2$ waveplate with its optic axis oriented at $5\pi/8 = 112.5^\circ$.

Solution to Exercise 1.28.

$$\hat{H}_2 \simeq \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

Solution to Exercise 1.29. We begin by writing the observable operator in the Dirac notation according to the definition (1.12):

$$(1) |H\rangle\langle H| + (-1)|V\rangle\langle V|. \quad (\text{S1.18})$$

This is equivalent to the Pauli operator $\hat{\sigma}_z$ [see Eq. (refpaulidefnDiracc)].

Similarly, using Table 1.1, we find for the diagonal basis measurement:

$$|+\rangle\langle +| - |-\rangle\langle -| \simeq \frac{1}{2} \begin{pmatrix} 1 & \\ & 1 \end{pmatrix} (1 \ 1) - \frac{1}{2} \begin{pmatrix} 1 & \\ & -1 \end{pmatrix} (1 \ -1) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \hat{\sigma}_x \quad (\text{S1.19})$$

and for the circular basis

$$|R\rangle\langle R| - |L\rangle\langle L| \simeq \frac{1}{2} \begin{pmatrix} 1 & \\ & i \end{pmatrix} (1 \ -i) - \frac{1}{2} \begin{pmatrix} 1 & \\ & -i \end{pmatrix} (1 \ i) = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} = \hat{\sigma}_y. \quad (\text{S1.20})$$

Solution to Exercise 1.30.

- a) The observable operator \hat{V} is given by Eq. (1.12). Because the eigenvalues of an observable are real (i.e. $v_i^* = v_i$), the adjoint operator is the same:

$$\hat{V}^\dagger = \sum_i v_i |v_i\rangle\langle v_i| = \hat{V}.$$

- b) This follows from the spectral theorem (Ex. A.60).

Solution to Exercise 1.31. We will begin with the Pauli matrix

$$\hat{\sigma}_x \simeq \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

We are looking for the eigenvalues and eigenvectors of this matrix (see e.g. the solution to Ex. A.64 for more details on this procedure). The characteristic equation takes the form

$$|\hat{\sigma}_x - v\hat{\mathbf{1}}| = \begin{vmatrix} -v & 1 \\ 1 & -v \end{vmatrix} = v^2 - 1 = 0$$

By solving for v , we find that our eigenvalues are $v_{1,2} = \pm 1$.

Now we find the eigenvector $|v\rangle \simeq \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$ associated with each of these eigenvalues by solving the equation $(\hat{\sigma}_x - v\hat{\mathbf{1}})|v\rangle = 0$. This equation becomes

$$\begin{pmatrix} -v & 1 \\ 1 & -v \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix},$$

from which, for $v_1 = 1$, we find $\alpha = \beta$. Also, we apply the normalization condition $\alpha^2 + \beta^2 = 1$ to determine a normalized eigenvector

$$|v_1\rangle \simeq \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \simeq |+\rangle. \quad (\text{S1.21})$$

Using the same procedure for the $v_2 = -1$ we obtain

$$|v_2\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} \simeq |-\rangle. \quad (\text{S1.22})$$

Now, we follow the same procedure to calculate the eigenvectors and eigenbasis for the other two Pauli matrices. For $\hat{\sigma}_y \simeq \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$, we get $v_{1,2} = \pm 1$ and

$$|v_1\rangle \simeq \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ i \end{pmatrix} \simeq |R\rangle; \quad |v_2\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -i \end{pmatrix} \simeq |L\rangle. \quad (\text{S1.23})$$

The matrix $\hat{\sigma}_z \simeq \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ is already diagonal, so $v_{1,2} = \pm 1$ and

$$|v_1\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \simeq |H\rangle; \quad |v_2\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \simeq |V\rangle.$$

These results are in agreement with the alternative definition of the Pauli matrices found in Ex. 1.29.

Note that in all three cases the matrix representations for the Pauli operators *in their own eigenbases* consist of the eigenvalues placed along the diagonal:

$$\hat{\sigma}_i = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad (\text{S1.24})$$

Solution to Exercise 1.32.

a) From Eq. (B.1) we may write that the expectation value is given by

$$\langle V \rangle = \sum_{i=1}^N \text{pr}_i v_i \quad (\text{S1.25})$$

where v_i is the value returned by the measurement and pr_i is the probability to detect $|\psi\rangle$ in the state $|v_i\rangle$. The latter equals

$$\text{pr}_i = |\langle v_i | \psi \rangle|^2 = \langle \psi | v_i \rangle \langle v_i | \psi \rangle \quad (\text{S1.26})$$

and hence

$$\begin{aligned}\langle V \rangle &= \sum_{i=1}^N v_i \langle \psi | v_i \rangle \langle v_i | \psi \rangle \\ &= \langle \psi | \left(\sum_{i=1}^N v_i |v_i\rangle \langle v_i| \right) | \psi \rangle\end{aligned}\tag{S1.27}$$

$$\stackrel{(1.12)}{=} \langle \psi | \hat{V} | \psi \rangle.\tag{S1.28}$$

b) Similarly to part (a),

$$\langle \Delta V^2 \rangle = \sum_i \text{pr}_i (v_i - \langle V \rangle)^2.\tag{S1.29}$$

Transforming the operator in the right-hand side of Eq. (1.15), we have

$$(\hat{V} - \langle V \rangle \hat{\mathbf{1}})^2 = \left\{ \sum_i [(v_i - \langle V \rangle) |v_i\rangle \langle v_i|] \right\}^2\tag{S1.30}$$

$$= \sum_{i,j} [(v_i - \langle V \rangle)(v_j - \langle V \rangle) |v_i\rangle \langle v_i| v_j\rangle \langle v_j|]\tag{S1.31}$$

$$= \sum_i [(v_i - \langle V \rangle)^2 |v_i\rangle \langle v_i|].\tag{S1.32}$$

The quantum mean value of this operator is then

$$\langle \psi | (\hat{V} - \langle V \rangle \hat{\mathbf{1}})^2 | \psi \rangle = \sum_i \langle \psi | v_i \rangle \langle v_i | \psi \rangle (v_i - \langle V \rangle)^2 = \sum_i \text{pr}_i (v_i - \langle V \rangle)^2,$$

which is the same as the right-hand side of Eq. (S1.29).

To prove Eq. (1.16), we utilize the result of Ex. B.2 to argue that

$$\langle \Delta V^2 \rangle = \sum_i \text{pr}_i v_i^2 - \langle V \rangle^2.\tag{S1.33}$$

The first term in the expression above is the expectation value of operator \hat{V}^2 .

Solution to Exercise 1.34. The experiment in question is equivalent to measuring observable $\hat{\sigma}_z$ N times and taking the sum of all the results. The statistics of such summation has been calculated in Ex. B.5. Applying the result of Ex. 1.33, we find that the expectation value is $N \langle \sigma_z \rangle = 0$ and the uncertainty is $\sqrt{N} \sqrt{\langle \Delta \sigma_z^2 \rangle} = \sqrt{N}$.

Solution to Exercise 1.35. If $|\psi\rangle$ is an eigenstate of the operator \hat{V} , we have $\hat{V}|\psi\rangle = v|\psi\rangle$ and $\hat{V}^2|\psi\rangle = v^2|\psi\rangle$. Therefore

$$\langle \Delta \hat{V}^2 \rangle = \langle \psi | \hat{V}^2 | \psi \rangle - \langle \psi | \hat{V} | \psi \rangle^2 = v^2 \langle \psi | \psi \rangle - (v \langle \psi | \psi \rangle)^2 = v^2 - v^2 = 0.$$

Conversely, suppose that the uncertainty of measuring the observable \hat{V} in the state $|\psi\rangle$ vanishes. Denoting $\hat{V}|\psi\rangle \equiv |\phi\rangle$, we write

$$\langle \Delta \hat{V}^2 \rangle = \langle \psi | \hat{V}^2 | \psi \rangle - \langle \psi | \hat{V} | \psi \rangle^2 = \langle \phi | \phi \rangle - \langle \psi | \phi \rangle^2,$$

where in the last equality we have utilized the fact that \hat{V} , as an observable, is Hermitian, so $\langle \psi | \hat{V}^2 | \psi \rangle = \langle \psi | \hat{V}^\dagger \hat{V} | \psi \rangle = \langle \phi | \phi \rangle$. By assumption, $\langle \Delta \hat{V}^2 \rangle = 0$, so we have

$$\langle \phi | \phi \rangle = \langle \psi | \phi \rangle^2. \quad (\text{S1.34})$$

Because the state $|\psi\rangle$ is normalized, we can rewrite Eq. (S1.34) as

$$\langle \psi | \psi \rangle \langle \phi | \phi \rangle = \langle \psi | \phi \rangle^2.$$

We now notice that the above equation saturates the Cauchy-Schwartz inequality (A.10). As determined in Ex. A.26, this can happen if and only if states $|\psi\rangle$ and $|\phi\rangle$ are collinear, i.e. $|\phi\rangle = \hat{V}|\psi\rangle = v|\psi\rangle$.

Solution to Exercise 1.36.

If both operators are simultaneously diagonalizable, we can present them in the form $\hat{A} = \sum_i A_i |v_i\rangle \langle v_i|$ and $\hat{B} = \sum_i B_i |v_i\rangle \langle v_i|$. Then:

$$\hat{A}\hat{B} = \sum_{ij} A_i B_j |v_i\rangle \underbrace{\langle v_i | v_j \rangle}_{\delta_{ij}} \langle v_j| = \sum_i A_i B_i |v_i\rangle \langle v_i| = \hat{B}\hat{A}. \quad (\text{S1.35})$$

Let us now prove the converse statement. Consider one of \hat{A} 's eigenvectors $|v_1\rangle$:

$$\hat{A}|v_1\rangle = v_1|v_1\rangle \quad (\text{S1.36})$$

Multiply both sides by \hat{B} on the left:

$$\hat{B}\hat{A}|v_1\rangle = v_1\hat{B}|v_1\rangle \quad (\text{S1.37})$$

Commuting the operators in the left-hand side above, we have

$$\hat{A}(\hat{B}|v_1\rangle) = v_1(\hat{B}|v_1\rangle), \quad (\text{S1.38})$$

so $\hat{B}|v_1\rangle$ must be an eigenstate of \hat{A} with the eigenvalue A_1 . If the eigenvalue v_1 is non-degenerate, this is only possible if $\hat{B}|v_1\rangle$ is proportional to $|v_1\rangle$ (Ex. A.66), which means that $|v_1\rangle$ is an eigenstate of \hat{B} .

Now let us consider the case of v_1 being degenerate. As we know from Ex. A.70, eigenstates of \hat{A} with eigenvalue v_1 form a subspace (which we shall call \mathbb{V}'). Moreover, Eq. (S1.38) tells us that operator \hat{B} maps any state in \mathbb{V}' onto another state in \mathbb{V}' .

Because \hat{B} is a Hermitian operator in \mathbb{V}' , it diagonalizes in this subspace. That is, there exists an orthonormal basis in \mathbb{V}' consisting of eigenvectors of \hat{B} . But because \mathbb{V}' only contains eigenvectors of \hat{A} , each element of this basis is a simultaneous eigenvector of both operators.

The same procedure can be applied to each of the subspaces associated with the eigenvalues of operator \hat{A} .

Solution to Exercise 1.37.

$$\begin{aligned}
\langle [\hat{A}, \hat{B}] \rangle &= \langle \psi | \hat{A} \hat{B} | \psi \rangle - \langle \psi | \hat{B} \hat{A} | \psi \rangle \\
&= \langle \psi | \hat{A} \hat{B} | \psi \rangle - \langle \psi | \hat{B}^\dagger \hat{A}^\dagger | \psi \rangle \quad [\text{because } \hat{A} \text{ and } \hat{B} \text{ are Hermitian}] \\
&= \langle \psi | \hat{A} \hat{B} | \psi \rangle - \langle \psi | \hat{A} \hat{B} | \psi \rangle^* \quad [\text{by Eq. (A.37)}] \\
&= \langle \hat{A} \hat{B} \rangle - \langle \hat{A} \hat{B} \rangle^* \\
&= 2i \text{Im} \langle \hat{A} \hat{B} \rangle \quad [\text{because } z - z^* = 2i \text{Im} z \text{ for any complex } z]
\end{aligned}$$

Similarly:

$$\begin{aligned}
\langle \{\hat{A}, \hat{B}\} \rangle &= \langle \psi | \hat{A} \hat{B} | \psi \rangle + \langle \psi | \hat{A} \hat{B} | \psi \rangle^* \\
&= \langle \hat{A} \hat{B} \rangle + \langle \hat{A} \hat{B} \rangle^* \\
&= 2 \text{Re} \langle \hat{A} \hat{B} \rangle
\end{aligned}$$

Finally,

$$|\langle [\hat{A}, \hat{B}] \rangle|^2 = 4 (\text{Im} \langle \hat{A} \hat{B} \rangle)^2 \leq 4 (\text{Im} \langle \hat{A} \hat{B} \rangle)^2 + 4 (\text{Re} \langle \hat{A} \hat{B} \rangle)^2 = 4 |\langle \hat{A} \hat{B} \rangle|^2. \quad (\text{S1.39})$$

Solution to Exercise 1.38. The left-hand side of the Cauchy-Schwarz inequality

$$\langle a | a \rangle \langle b | b \rangle \geq |\langle a | b \rangle|^2 \quad (\text{S1.40})$$

for $|a\rangle = \hat{A}|\psi\rangle$ and $|b\rangle = \hat{B}|\psi\rangle$, where \hat{A} and \hat{B} are Hermitian operators, takes the form

$$\langle a | a \rangle \langle b | b \rangle = \langle \psi | \hat{A}^\dagger \hat{A} | \psi \rangle \langle \psi | \hat{B}^\dagger \hat{B} | \psi \rangle = \langle \psi | \hat{A}^2 | \psi \rangle \langle \psi | \hat{B}^2 | \psi \rangle. \quad (\text{S1.41})$$

Similarly, the right-hand side of Eq. (S1.40) becomes

$$|\langle a | b \rangle|^2 = |\langle \psi | \hat{A} \hat{B} | \psi \rangle|^2, \quad (\text{S1.42})$$

so inequality (S1.40) takes the form of Eq. (1.20).

Solution to Exercise 1.39. Because $\langle A \rangle = \langle B \rangle = 0$, we have $\langle \Delta \hat{A}^2 \rangle = \langle A^2 \rangle$ and $\langle \Delta \hat{B}^2 \rangle = \langle B^2 \rangle$, so the uncertainty principle (1.21) takes the form:

$$\langle \psi | \hat{A}^2 | \psi \rangle \langle \psi | \hat{B}^2 | \psi \rangle \geq \frac{1}{4} |\langle \psi | [\hat{A}, \hat{B}] | \psi \rangle| \quad (\text{S1.43})$$

This result obtains immediately from Eqs. (1.19) and (1.20).

Solution to Exercise 1.40. Let us define operators $\hat{A}' = \hat{A} - \langle \hat{A} \rangle$ and $\hat{B}' = \hat{B} - \langle \hat{B} \rangle$. The expectation values of these observables vanish, so we can use the “simplified” uncertainty principle from the previous exercise to write

$$\langle \hat{A}'^2 \rangle \langle \hat{B}'^2 \rangle \geq \frac{1}{4} |\langle [\hat{A}', \hat{B}'] \rangle|^2. \quad (\text{S1.44})$$

At the same time, we have

$$\begin{aligned}\langle \Delta A^2 \rangle &= \langle (A - \langle A \rangle)^2 \rangle = \langle A'^2 \rangle; \\ \langle \Delta B^2 \rangle &= \langle (B - \langle B \rangle)^2 \rangle = \langle B'^2 \rangle\end{aligned}\quad (\text{S1.45})$$

and

$$\begin{aligned}[\hat{A}', \hat{B}'] &= \hat{A}'\hat{B}' - \hat{B}'\hat{A}' \\ &= (\hat{A} - \langle \hat{A} \rangle)(\hat{B} - \langle \hat{B} \rangle) - (\hat{B} - \langle \hat{B} \rangle)(\hat{A} - \langle \hat{A} \rangle) \\ &= \hat{A}\hat{B} - \langle \hat{A} \rangle \hat{B} - \hat{A} \langle \hat{B} \rangle + \langle \hat{A} \rangle \langle \hat{B} \rangle - \hat{B}\hat{A} + \hat{B} \langle \hat{A} \rangle + \langle \hat{B} \rangle \hat{A} - \langle \hat{B} \rangle \langle \hat{A} \rangle \\ &= \hat{A}\hat{B} - \hat{B}\hat{A} \\ &= [\hat{A}, \hat{B}].\end{aligned}\quad (\text{S1.46})$$

Substituting Eqs. (S1.45) and (S1.46) into Eq. (S1.44), we obtain

$$\langle \Delta \hat{A}^2 \rangle \langle \Delta \hat{B}^2 \rangle \geq \frac{1}{4} |\langle [\hat{A}, \hat{B}] \rangle|^2. \quad (\text{S1.47})$$

The uncertainty principle would not remain valid if the commutator of \hat{A} and \hat{B} were replaced by the anticommutator or product of these operators because in this case Eq. (S1.46) would no longer apply.

Solution to Exercise 1.41.

$$\langle \Delta \hat{A}^2 \rangle \langle \Delta \hat{B}^2 \rangle \geq \frac{1}{4} |\langle [\hat{A}, \hat{B}] \rangle|^2 = \frac{1}{4} |\langle \epsilon \hat{\mathbf{1}} \rangle|^2 = \frac{1}{4} |\epsilon|^2$$

Solution to Exercise 1.42.

a)

$$\langle \hat{\sigma}_x \rangle = \langle H | \hat{\sigma}_x | H \rangle = (1 \ 0) \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = 0; \quad (\text{S1.48})$$

$$\langle \hat{\sigma}_y \rangle = \langle H | \hat{\sigma}_y | H \rangle = (1 \ 0) \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = 0; \quad (\text{S1.49})$$

$$\begin{aligned}\langle \Delta \hat{\sigma}_x^2 \rangle &= \langle H | \hat{\sigma}_x^2 | H \rangle - (\langle H | \hat{\sigma}_x | H \rangle)^2 \\ &= (1 \ 0) \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} - 0 = 1;\end{aligned}$$

$$\begin{aligned}\langle \Delta \hat{\sigma}_y^2 \rangle &= \langle H | \hat{\sigma}_y^2 | H \rangle - \langle H | \hat{\sigma}_y | H \rangle^2 \\ &= (1 \ 0) \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} - 0 = 1.\end{aligned}$$

On the other hand, we know from Ex. A.78 that $[\hat{\sigma}_x, \hat{\sigma}_y] = 2i\hat{\sigma}_z$ so

$$\langle [\hat{\sigma}_x, \hat{\sigma}_y] \rangle = \langle H | 2i\hat{\sigma}_z | H \rangle = (1 \ 0) \begin{pmatrix} 2i & 0 \\ 0 & -2i \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = 2i.$$

b) The uncertainty principle takes the form

$$\langle \Delta \hat{\sigma}_x^2 \rangle \langle \Delta \hat{\sigma}_y^2 \rangle \geq \frac{1}{4} |\langle [\hat{\sigma}_x, \hat{\sigma}_y] \rangle|^2.$$

Both sides of the inequality equal 1.

c) The uncertainty product can vanish for any state in which the expectation value of $\hat{\sigma}_z$ is zero. For example, if $|\psi\rangle = |+\rangle$, observable $\hat{\sigma}_x$ has a certain value of $+1$, and hence the uncertainty product is zero.

Solution to Exercise 1.43. According to Eq. (1.25),

$$|\psi(t)\rangle = \frac{(e^{-iE_1t/\hbar} |E_1\rangle + e^{-iE_2t/\hbar} |E_2\rangle)}{\sqrt{2}} \quad (\text{S1.50})$$

$$= e^{-iE_1t/\hbar} \frac{(|E_1\rangle + e^{-i(E_2-E_1)t/\hbar} |E_2\rangle)}{\sqrt{2}}. \quad (\text{S1.51})$$

Neglecting the overall phase factor, state $|\psi(t)\rangle$ becomes physically equivalent to $(|E_1\rangle - |E_2\rangle)/\sqrt{2}$ when $e^{-i(E_2-E_1)t/\hbar} = -1$, or $|E_2 - E_1|t/\hbar = \pi$.

Solution to Exercise 1.44.

a) Let $\{|E_k\rangle\}$ be the energy eigenbasis. From Eq. (1.25) we know that $\hat{U} |E_k\rangle = e^{-iE_k t/\hbar} |E_k\rangle$. The matrix elements of the evolution operator are therefore

$$U_{ji} = \langle E_j | \hat{U} | E_k \rangle = e^{-iE_k t/\hbar} \langle E_j | E_k \rangle = e^{-iE_k t/\hbar} \delta_{jk}.$$

Hence

$$\hat{U} \simeq \begin{pmatrix} e^{-iE_1t/\hbar} & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & e^{-iE_Nt/\hbar} \end{pmatrix}. \quad (\text{S1.52})$$

b) This matrix can be rewritten in the Dirac notation using Eq. (A.24) as

$$\hat{U} = \sum_k e^{-iE_k t/\hbar} |E_k\rangle \langle E_k|. \quad (\text{S1.53})$$

Comparing this with the equation (1.26) for the Hamiltonian and the definition (A.49) of operator functions, we find that $\hat{U}(t) = e^{-i\hat{H}t/\hbar}$. The Hamiltonian operator \hat{H} corresponds to a physical observable, energy, and is thus Hermitian. The Schrödinger evolution operator, $e^{-i\hat{H}t/\hbar}$ must then be unitary according to Ex. A.92.

Solution to Exercise 1.46. According to the result of Ex. A.96:

$$\frac{d}{dt} e^{-\frac{i}{\hbar} \hat{H} t} |\psi(0)\rangle = -\frac{i}{\hbar} \hat{H} e^{-\frac{i}{\hbar} \hat{H} t} |\psi(0)\rangle = -\frac{i}{\hbar} \hat{H} |\psi(t)\rangle,$$

which is consistent with the Schrödinger equation (1.31).

Solution to Exercise 1.47.

- a) *Method I.* The eigenstates of the operator $\hat{\sigma}_z$ are $|H\rangle$ and $|V\rangle$, with the corresponding eigenvalues ± 1 (Ex. 1.29), which means that the energy eigenvalues are $E_H = \hbar\omega$ and $E_V = -\hbar\omega$. The initial state $|\psi(0)\rangle = |H\rangle$ is an eigenstate of the Hamiltonian (and hence a stationary state), and evolves according to

$$|\psi(t)\rangle \stackrel{(1.28)}{=} e^{-\frac{i}{\hbar} E_H t} |H\rangle = e^{-i\omega t} |H\rangle.$$

The initial state $|\psi(0)\rangle = |+\rangle = \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle)$, and hence

$$|\psi(t)\rangle \stackrel{(1.28)}{=} \frac{1}{\sqrt{2}}(e^{-\frac{i}{\hbar} E_H t} |H\rangle + e^{-\frac{i}{\hbar} E_V t} |V\rangle) = \frac{1}{\sqrt{2}}(e^{-i\omega t} |H\rangle + e^{i\omega t} |V\rangle).$$

Method II. Since $\hat{\sigma}_z = |H\rangle\langle H| - |V\rangle\langle V|$, the evolution operator is (cf. Ex. A.94)

$$\hat{U}(t) = e^{-i\omega \hat{\sigma}_z t} = e^{-i\omega t} |H\rangle\langle H| + e^{i\omega t} |V\rangle\langle V|. \quad (\text{S1.54})$$

By applying Eq. (1.29) we have for a photon initially in $|\psi(0)\rangle = |H\rangle$:

$$\begin{aligned} |\psi(t)\rangle &= (e^{-i\omega t} |H\rangle\langle H| + e^{i\omega t} |V\rangle\langle V|) |H\rangle \\ &= e^{-i\omega t} |H\rangle. \end{aligned}$$

For the initial state $|\psi(0)\rangle = |+\rangle$:

$$\begin{aligned} |\psi(t)\rangle &= (e^{-i\omega t} |H\rangle\langle H| + e^{i\omega t} |V\rangle\langle V|) \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle) \\ &= \frac{1}{\sqrt{2}}(e^{-i\omega t} |H\rangle + e^{i\omega t} |V\rangle). \end{aligned}$$

Method III. Let

$$|\psi(t)\rangle \simeq \begin{pmatrix} \psi_H(t) \\ \psi_V(t) \end{pmatrix} \quad (\text{S1.55})$$

in the canonical basis. The matrix of the Hamiltonian is

$$\hat{H} \simeq \hbar\omega \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

and the Schrödinger equation becomes

$$\frac{d}{dt} \begin{pmatrix} \psi_H(t) \\ \psi_V(t) \end{pmatrix} = -i\omega \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} \psi_H(t) \\ \psi_V(t) \end{pmatrix},$$

or

$$\frac{d}{dt} \begin{pmatrix} \psi_H(t) \\ \psi_V(t) \end{pmatrix} = -i\omega \begin{pmatrix} \psi_H(t) \\ -\psi_V(t) \end{pmatrix}.$$

This expression means that the differential equation must hold for each row of the matrices in the left- and right-hand side, so we can rewrite it as a system of ordinary differential equations:

$$\begin{cases} \dot{\psi}_H(t) = -i\omega\psi_H(t) \\ \dot{\psi}_V(t) = i\omega\psi_V(t) \end{cases}$$

which has the following solution:

$$\begin{cases} \psi_H(t) = Ae^{-i\omega t} \\ \psi_V(t) = Be^{i\omega t} \end{cases}$$

The coefficients A and B are obtained from the initial conditions. If the initial state is $|H\rangle \simeq \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, then we have $A = 1, B = 0$ and thus

$$|\psi(t)\rangle \simeq \begin{pmatrix} e^{-i\omega t} \\ 0 \end{pmatrix} \simeq e^{-i\omega t} |H\rangle.$$

If the initial state is $|+\rangle \simeq \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}$, then we have $A = B = \frac{1}{\sqrt{2}}$ and thus

$$|\psi(t)\rangle \simeq \frac{1}{\sqrt{2}} \begin{pmatrix} e^{-i\omega t} \\ e^{i\omega t} \end{pmatrix},$$

in agreement with the answer obtained using the other two methods.

- b) *Method I.* The eigenstates of the Hamiltonian are now $|+\rangle$ and $|-\rangle$, with the corresponding eigenvalues $E_{\pm} = \pm\hbar\omega$. The initial state $|H\rangle$ decomposes according to $|\psi(0)\rangle = \frac{1}{\sqrt{2}}(|+\rangle + |-\rangle)$, and evolves according to

$$\begin{aligned} |\psi(t)\rangle &= \frac{1}{\sqrt{2}}(e^{-\frac{i}{\hbar}E_+t} |+\rangle + e^{-\frac{i}{\hbar}E_-t} |-\rangle) \\ &= \frac{1}{\sqrt{2}}(e^{-i\omega t} |+\rangle + e^{i\omega t} |-\rangle) \\ &= \frac{1}{2}[e^{-i\omega t}(|H\rangle + |V\rangle) + e^{i\omega t}(|H\rangle - |V\rangle)] \\ &= \cos \omega t |H\rangle - i \sin \omega t |V\rangle. \end{aligned}$$

The initial state $|+\rangle$ is an eigenstate of the Hamiltonian:

$$|\psi(t)\rangle \stackrel{(1.28)}{=} e^{-\frac{i}{\hbar}E_+t} |+\rangle = e^{-i\omega t} |+\rangle = \frac{1}{\sqrt{2}}e^{-i\omega t}(|H\rangle + |V\rangle).$$

Method II. The evolution operator is now

$$\hat{U}(t) = e^{-i\omega\hat{\sigma}_x} = e^{-i\omega t} |+\rangle\langle +| + e^{i\omega t} |-\rangle\langle -|. \quad (\text{S1.56})$$

The time evolution for a photon initially in $|\psi(0)\rangle = |H\rangle$ is

$$\begin{aligned}
|\psi(t)\rangle &= \hat{U}(t)|H\rangle \\
&= [e^{-i\omega t}|+\rangle\langle+| + e^{i\omega t}|-\rangle\langle-|] \frac{1}{\sqrt{2}}(|+\rangle + |-\rangle) \\
&= \frac{1}{\sqrt{2}}(e^{-i\omega t}|+\rangle + e^{i\omega t}|-\rangle) \\
&= \cos \omega t |H\rangle - i \sin \omega t |V\rangle.
\end{aligned}$$

For the initial state $|\psi(0)\rangle = |+\rangle$:

$$|\psi(t)\rangle = (e^{-i\omega t}|+\rangle\langle+| + e^{i\omega t}|-\rangle\langle-|)|+\rangle e^{-i\omega t}|+\rangle.$$

Method III. In order to apply the Schrödinger equation technique, we again decompose $|\psi(t)\rangle$ according to Eq. (S1.55). The matrix of the Hamiltonian takes the form

$$\hat{H} \simeq \hbar\omega \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

and the Schrödinger equation takes the form

$$\frac{d}{dt} \begin{pmatrix} \psi_H(t) \\ \psi_V(t) \end{pmatrix} = -i\omega \begin{pmatrix} \psi_V(t) \\ \psi_H(t) \end{pmatrix}.$$

The system of equations for the state components is

$$\begin{cases} \dot{\psi}_H(t) = -i\omega\psi_V(t) \\ \dot{\psi}_V(t) = -i\omega\psi_H(t) \end{cases}.$$

In order to solve this system we can, for example, take the derivative of both sides of the first equation and substitute $\dot{\psi}_V(t)$ from the second one:

$$\ddot{\psi}_H(t) = -i\omega\dot{\psi}_V(t) = -\omega^2\psi_H(t).$$

This equation has solution

$$\psi_H(t) = Ae^{i\omega t} + Be^{-i\omega t}$$

and, accordingly,

$$\psi_V(t) = \dot{\psi}_H(t)/(-i\omega) = -Ae^{i\omega t} + Be^{-i\omega t}.$$

For the initial state $|H\rangle$, we have $\psi_H(0) = 1$, $\psi_V(0) = 0$, hence $A = B = 1/2$ and thus

$$|\psi(t)\rangle \simeq \frac{1}{2} \begin{pmatrix} e^{i\omega t} + e^{-i\omega t} \\ -e^{i\omega t} + e^{-i\omega t} \end{pmatrix} = \begin{pmatrix} \cos \omega t \\ -i \sin \omega t \end{pmatrix}.$$

For the initial state $|+\rangle$, we have $\psi_H(0) = \psi_V(0) = 1/\sqrt{2}$, hence $A = 0$, $B = \frac{1}{\sqrt{2}}$ and thus

$$|\psi(t)\rangle \simeq \frac{1}{\sqrt{2}} \begin{pmatrix} e^{-i\omega t} \\ e^{-i\omega t} \end{pmatrix} \simeq e^{-i\omega t} |+\rangle.$$

Solution to Exercise 1.48. Polarization state transformations by half-waveplates at 0 and 45° are given by operators $-|H\rangle\langle H| + |V\rangle\langle V|$ and $-(|+\rangle\langle +|) + (|-\rangle\langle -|)$, respectively (see Ex. 1.24). Comparing these with the evolution operators (S1.54) and (S1.56), respectively, we see that they become identical, up to an overall phase factor, when $\omega t_{\text{HWP}} = \pi/2$ in both cases. The quarter-wave plate corresponds to the evolution for a time period that is one-half of that for a half-wave plate, i.e. $\omega t_{\text{QWP}} = \pi/4$.