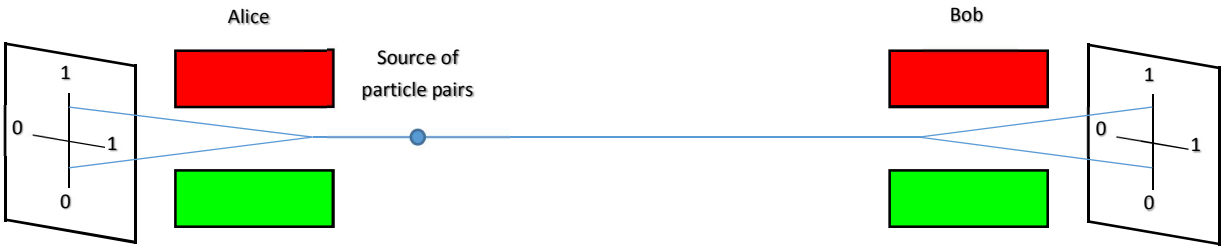
Basics



1. A) Suppose we have two entangled spin-½ particles (particles A and B) described in the Z basis by the state $|\Psi_{AB}\rangle = 1/\sqrt{2}[|\uparrow_A\rangle_Z|\downarrow_B\rangle_Z - |\downarrow_A\rangle_Z|\uparrow_B\rangle_Z]$. Given that $|\uparrow_A\rangle_Z = 1/\sqrt{2}\,(|\uparrow_A\rangle_X + |\downarrow_A\rangle_X)$ and $|\downarrow_A\rangle_Z = 1/\sqrt{2}\,(|\uparrow_A\rangle_X - |\downarrow_A\rangle_X)$, write down the entangled state of the two particles in the X basis and simplify the expression.

1. B) How does this expression for the state in the X basis compare to the state in the Z basis?

Throughout the "Basics" section, we will consider the case of entangled spin-½ particles (particles A and B) described by the state discussed above. All measurements refer to measurements of spin performed using a Stern-Gerlach Apparatus (SGA) and a screen. The SGA consists of a region of non-uniform magnetic field along a given axis (either along the Z axis or X axis). Measurement of the spin state of the particle along the axis of the SGA can then be made by using a screen to detect how the particle was deflected (e.g., see the figure above). Detection of the particle on the screen produces a flash (the flash may be shifted up/down or left/right depending on the SGAs' magnetic field gradient and this particle's spin state into which the system collapses upon measurement). In general, spin-½ particles can separate into two distinct streams, e.g., one deflected upwards (which we call measurement outcome 1), one deflected downwards (which we call measurement outcome 0) along the axis.

2. A) Particle A's spin state is measured along the Z axis. In what basis will the outcome of the measurement of particle B's spin state be deterministic (i.e., the outcome is pre-determined before measurement)?

(a) The X basis
(b) The Z basis
(c) Either X or Z basis, both yield deterministic outcomes
(d) None of the above. In quantum mechanics, the outcomes are never deterministic.

2. B) Explain your reasoning for answer 2A)

3. Consider the following statements by two students:
Student 1: "The answer to question 2 A) must be option (b). The measurement of particle A along the Z axis collapses the state $|\Psi_{AB}\rangle = 1/\sqrt{2}[|\uparrow_A\rangle_Z|\downarrow_B\rangle_Z - |\downarrow_A\rangle_Z|\uparrow_B\rangle_Z]$ into either $|\uparrow_A\rangle_Z|\downarrow_B\rangle_Z$ or $|\downarrow_A\rangle_Z|\uparrow_B\rangle_Z$. Therefore, the measurement of particle A's spin state, as either $|\uparrow_A\rangle_Z$ or $|\downarrow_A\rangle_Z$, can be used to infer that measurement of particle B's spin state will definitely be either $|\downarrow_B\rangle_Z$ or $|\uparrow_B\rangle_Z$, respectively.

Student 2: "No, The answer to question 2 A) must be option (d). A fundamental axiom of quantum mechanics is that the outcome of a measurement can never be predicted ahead of time.

Do you agree with "Student 1", "Student 2" or neither? Explain your reasoning.

4. A) Particle A's spin state is measured in the Z basis as $|\uparrow_A\rangle_Z$. Which one of the following is a good prediction of the measurement for particle B's spin state in the Z basis after Particle A's spin measurement?

(a) $|\uparrow_B\rangle_X$
(b) $|\downarrow_B\rangle_X$
(c) $|\uparrow_B\rangle_Z$
(d) $|\downarrow_B\rangle_Z$
(e) We cannot predict Particle B's spin state from the knowledge of particle A's spin state even if the chosen basis is the same.

4. B) Explain how you made this prediction.

5. Particle A's spin state is measured in the Z basis as $|\uparrow_A\rangle_Z$. Which one of the following is a good prediction of the measurement for particle B's spin state in the X basis after Particle A's spin measurement?

(a) $|\uparrow_B\rangle_X$
(b) $|\downarrow_B\rangle_X$
(c) Either $|\uparrow_B\rangle_X$ or $|\downarrow_B\rangle_X$ with equal likelihood
(d) None of the above

6. A) Particle A's spin state is measured in the Z basis as $|\uparrow_A\rangle_Z$. What is the likelihood of measuring particle B's spin state in the X basis as $|\uparrow_B\rangle_X$?

(a) 100%
(b) 50%
(c) 25%
(d) 0%

6. B) Explain how this likelihood was found.

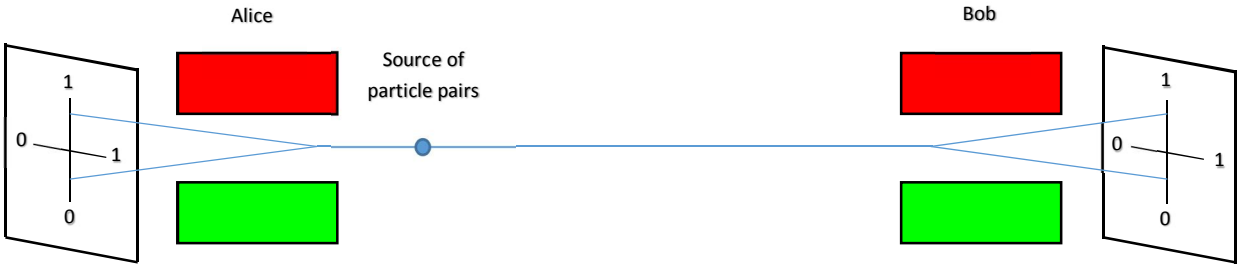
7. A) Suppose Particle B's spin was measured before any measurement was performed on particle A. What is the likelihood of measuring particle B in the Z basis as $|\uparrow_B\rangle_Z$.

(a) 100%
(b) 75%
(c) 50%
(d) 0%

7. B) Explain how you found this likelihood.

Secure Quantum Key Distribution with Entangled Spin ½ Particles

Acknowledgement: The simulations used in this tutorial were developed by Antje Kohnle (http://quantumphysics.iop.org). The protocol used in this tutorial is based on C. Bennett, G. Brassard and N. D. Mermin, Phys. Rev. Lett., 68, 557-559 (1992).



Goal: Learn a secure quantum mechanical protocol for generating a shared binary key over a public channel using an entangled state of two particles such that Alice and Bob will be able to tell if somebody was eavesdropping.

Alice and Bob want to generate a binary "key" (useful for encoding and decoding secret information) over a public channel (where a third party can eavesdrop on what is being sent). Since Alice and Bob cannot meet in person, they discuss the following protocol for generating such a key over a public channel (e.g. telephone, e-mail, etc). Their plan makes use of a source that produces two entangled spin-½ particles (ignore orbital angular momentum, assuming it is zero) in Alice's lab, two Stern-Gerlach Apparati (SGA) and two screens which act as measurement devices (the measurement of a particle at a particular point on the fluorescent screen is registered as a flash). The SGA consists of a region of non-uniform magnetic field along a given axis (either along the X axis or Z axis). Measurement of the spin state of the particle along the axis of the SGA can then be made by using a screen to detect how the particle was deflected (e.g., as shown in the Figure above). Detection of the particle on the screen produces a flash (the flash may be shifted up/down or left/right depending on the SGA's magnetic field gradient and the particle's spin state into which the system collapses upon measurement). In general, spin-½ particles can separate into two distinct streams, e.g., one deflected upwards (which we call measurement outcome 1) and one deflected downwards (which we call measurement outcome 0) along the axis determined by the magnetic field gradient of the SGA.

- A source generates a pair of entangled spin-½ particles in Alice's lab which move in opposite directions towards Alice's and Bob's SGAs (see figure).
- These two entangled particles A and B are described by the state $|\Psi_{AB}\rangle = 1/\sqrt{2}(|\uparrow_A\rangle|\downarrow_B\rangle - |\downarrow_A\rangle|\uparrow_B\rangle)$ (where A is the particle that moves towards the measuring screen in Alice's lab and B is the particle that moves towards the measuring screen in Bob's lab).
- Particle A in the entangled state passes through a SGA in Alice's lab which she randomly orients along one of two orthogonal axes, denoted X and Z, and she measures the deflection of the particle (up/down or left/right) and notes the orientation of her SGA (whether the direction of the magnetic field gradient is along the X or Z axis).
- Alice and Bob have decided that upward deflection on Alice's screen in the z direction will be noted as a "1" and deflection to the right on Alice's screen in the x direction will be noted as a "1". The other two deflections in her lab will be noted as "0" in their shared binary key.
- Particle B in the entangled state passes over the public channel to Bob's lab and through his SGA which he randomly orients along one of the two orthogonal axes (X and Z). Bob notes the deflection (up/down or left/right) and also notes the orientation of his SGA.

- After both Alice and Bob perform each measurement, they compare using a public channel the orientations of their SGAs (the direction of the magnetic field gradients) but not the observed deflection.
- If both Alice and Bob happened to use the same orientation for their SGAs for a particular measurement (had the same basis), Alice and Bob know with certainty what the other person obtained since their measurements are anti-correlated. In this case, Alice writes down her deflection measurement as the next bit of the binary key and Bob also records the opposite of the deflection on his screen (to match Alice's bit) as the next bit of the common shared binary key they generate (e.g. if Bob notes upward deflection in the Z direction and measures a 1 he records a 0 because that is what Alice must have recorded for her particle in an error-free measurement).
- If the comparison of Alice and Bob's SGA orientations over the public channel show that they did not use the same orientation or "basis" (i.e., their SGAs had different magnetic field gradients), they discard that bit (do not include it in their shared key).
- They perform this procedure many times to generate a shared key of the length they want.

For these first 10 questions, assume that no eavesdropping occurs during the key distribution (shared key generation over public channel using the protocol discussed above).

8. Bob uses a SGA oriented along the X axis and measures a 1. If Alice measures a 0, which one of the following is true?

(e) Alice must have an X oriented SGA.
(f) Alice must have a Z oriented SGA.
(g) Alice can have either an X or Z oriented SGA.
(h) None of the above.

9. Bob uses a SGA oriented along the X axis and measures a 1. If Alice measures a 1, which one of the following is true?

(a) Alice must have an X oriented SGA.
(b) Alice must have a Z oriented SGA.
(c) Alice can have either an X or Z oriented SGA.
(d) None of the above.

10. If Alice uses a SGA oriented along the Z axis and measures a 0, what is the likelihood that Bob measures a 1? Hint: Recall that Bob randomly orients his SGA either along the X or Z axis.

(a) 100% certainty
(b) 75% certainty
(c) 50% certainty
(d) 25% certainty

11. If Alice uses a SGA oriented along the Z axis and measures a 1, what is the likelihood that Bob measures a 1? Hint: Recall that Bob randomly orients his SGA either along the X or Z axis.

(a) 100% certainty
(b) 75% certainty
(c) 50% certainty
(d) 25% certainty

12. If Bob and Alice both use SGAs oriented along the Z axis, choose all of the following statements that are true:

(I) If Alice measures a 1, Bob **must** measure a 0.
(II) If Alice measures a 0, Bob **must** measure a 1.
(III) If Alice measures a 1, Bob may measure either a 1 or a 0.

(a) (I) only
(b) (III) only
(c) (I) and (II) only
(d) (II) and (III) only

13. Bob uses a SGA oriented along the X axis and Alice uses a SGA oriented along the Z axis, choose all of the following statements that are true:

(I) If Alice measures a 1, Bob **must** measure a 0.
(II) If Alice measures a 0, Bob **must** measure a 1.
(III) If Alice measures a 1, Bob may measure either a 1 or a 0.

(a) (I) only
(b) (III) only
(c) (I) and (II) only
(d) (II) and (III) only

14. Choose all of the following statements that are correct:

(I) If Bob measures a 1, he can always infer the measurement that Alice makes.
(II) If Bob measures a 0, he can always infer the measurement that Alice makes.
(III) If Alice and Bob both have their SGAs oriented in the same direction, Bob should be able to determine what Alice measures.

(a) (I) only
(b) (II) only
(c) (III) only
(d) (I) and (III) only

15. Assume Alice and Bob conduct a large number of measurements. Complete the following table by recording in the third column whether or not Bob knows with certainty what Alice measures from the knowledge of Alice's SGA orientation:

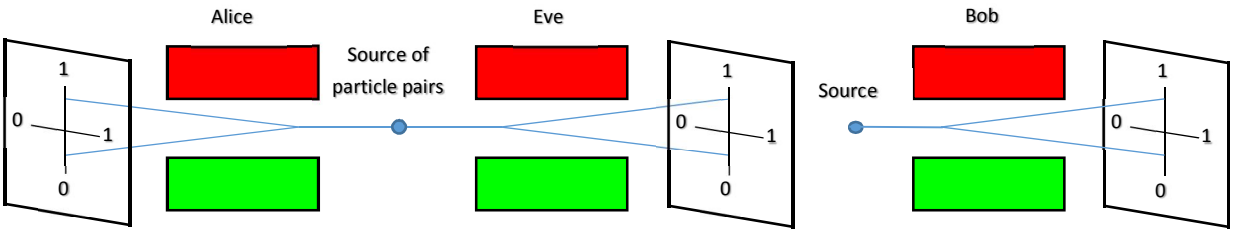
Alice's SGA Orientation	Bob's SGA Orientation	Bob is Certain or Uncertain
X axis	X axis	
	Z axis	
Z axis	X axis	
	Z axis	

16. When both Alice and Bob randomly orient their SGAs, what is the likelihood that Bob knows what Alice measures? Hint: Use the table you generated above.

(a) 100% certainty
(b) 75% certainty
(c) 50% certainty
(d) 25% certainty

17. Complete the following Table with the measurements made by Bob in each case (write 1, 0, or "– " where you are not certain because it could be either 1 or 0).

	Alice measures a 1				Alice measures a 0			
	Alice's SGA is along the X axis		Alice's SGA is along the Z axis		Alice's SGA is along the X axis		Alice's SGA is along the Z axis	
	Bob's SGA is along the X axis	Bob's SGA is along the Z axis	Bob's SGA is along the X axis	Bob's SGA is along the Z axis	Bob's SGA is along the X axis	Bob's SGA is along the Z axis	Bob's SGA is along the X axis	Bob's SGA is along the Z axis
Bob's measurement (1, 0, or -)								



Now let us assume that there is a third party, Eve, who is intercepting every particle in the entangled state being sent to Bob with her own SGA which she randomly orients along the X or Z direction (similar to the strategy used by Alice and Bob). Then, Eve immediately generates a replacement particle (unlike the entangled state) to send to Bob in its place. Let us assume that Eve can generate the replacement particle instantly and that she matches the particle that she intercepted (e.g., if Eve measures a 1 along the Z axis, she produces and sends a particle to Bob which is also in $|\uparrow_B\rangle_Z$ state). The following questions are based on these types of scenarios.

18. If Alice and Bob have their SGAs oriented along different axes for a measurement, which one of the following statements is true about what Eve will gain from this measurement.

(a) Eve will gain the next bit of the key if her SGA is oriented along the same axis as Alice's.
(b) Eve will gain the next bit of the key if her SGA is oriented along the same axis as Bob's.
(c) Eve will gain the next bit of the key regardless of the axis along which she orients her SGA.
(d) Eve cannot gain the next bit of the key because Alice and Bob will discard this measurement

Since Alice and Bob discard all measurements for which their SGAs are not oriented in the same direction, (either both in the Z direction or both in the X direction) nothing is gained from examining these cases. Therefore, we will ignore such cases for the remainder of this tutorial homework.

19. If Alice and Bob both have their SGAs oriented along the X axis for a measurement, which one of the following statements is true about whether Eve can be 100% sure about what Alice had noted as the corresponding bit of the key (after Alice and Bob inform each other of their SGA orientations over the public channel).

(a) Eve will be certain about the next bit of the key if her SGA is oriented along the X axis.
(b) Eve will be certain about the next bit of the key if her SGA is oriented along the Z axis.
(c) Eve will be certain about the next bit of the key regardless of the orientation of her SGA.
(d) Eve cannot be certain the next bit of the key because Alice and Bob will discard this measurement.

20. If Alice and Bob have their SGAs oriented along the Z axis and Eve has her SGA oriented along the Z axis, how does Eve's measurement compare to the one Bob would have performed had Eve not interfered?

(a) Eve's measurement is the same as the one Bob would have made. This situation is such that Eve's presence will go undetected.
(b) Eve's measurement is the opposite to the one Bob would have made (e.g., If Eve measures a 1 then Bob would measure a 0 and vice versa).
(c) Eve's measurement is either the same as or opposite to the one Bob would have made with equal likelihood.
(d) None of the above.

21. If Alice and Bob have their SGAs oriented along the Z axis and Eve has her SGA oriented along the X axis, how does Eve's measurement (i.e., 1 or 0) compare to the one Bob would have made had Eve not interfered?

(a) Eve's measurement is definitely the same as the one Bob would have made.
(b) Eve's measurement is opposite the one Bob would have made (e.g. if Eve measures a 1, Bob would have measured a 0 or vice versa).
(c) Eve's measurement is either the same as or opposite to the one Bob would have made with equal likelihood.
(d) None of the above.

22. Alice and Bob have their SGAs oriented along the X axis and Eve has her SGA oriented along the X axis. If Eve generates a replacement particle and sends it to Bob, as described above, what is the likelihood that Bob will make the same measurement that he would have without Eve's interference?

(a) 100%
(b) 75%
(c) 50%
(d) 25%

23. Alice and Bob have their SGAs oriented along the Z axis and Eve has her SGA oriented along the X axis. If Eve generates a replacement particle and sends it to Bob, as described above, what is the likelihood that Bob will make the same measurement that he would have without Eve's interference?

(a) 100%
(b) 50%
(c) 25%
(d) 0%

24. If both Alice and Bob have their SGAs oriented along the X axis, what is the likelihood that Bob will detect Eve's interference (their bits will not match), if Alice and Bob were to compare their records?

(a) 75%
(b) 50%
(c) 25%
(d) 0%

25. Complete the following table by entering the likelihood that Bob will detect Eve's interference (Alice and Bob's bits will not match) if Alice and Bob were to compare some bits, e.g., every 10^{th} bit, for each of the following cases.

Alice and Bob's SGA Orientation	Eve's SGA Orientation	Likelihood of Detecting Interference
X axis	X axis	
	Z axis	
Z axis	X axis	
	Z axis	

26. What is the overall likelihood that Bob will detect interference for a bit in the key (if he compares many bits with Alice) due to eavesdropping by Eve out of the cases in which Alice and Bob record the bit._____

27. Once the shared encryption key has been generated bit by bit using the above protocol, a small subset of bits, e.g., every 10^{th} bit is compared by Alice and Bob over a public channel (they discard these bits that they compare so that these bits are not part of the shared key generated). If there are significant inconsistencies between the bits that Alice and Bob compare, these discrepancies (e.g., if Alice has a 1 for a particular bit then Bob has a 0) may have arisen because

(I) Eve was eavesdropping and incorrectly replaced some of the particles that were meant for Bob.
(II) Alice must have written down incorrect bits.
(III) Bob must have written down incorrect bits.

(a) (I) only
(b) (II) only
(c) (III) only
(d) (II) and (III) only

While classically there is no secure way to share a key for encoding and decoding information using a public channel, the above quantum mechanical protocol can inform Alice and Bob if someone is eavesdropping. In case they detect eavesdropping, they can abort the key sharing process and try again at a later time when nobody is eavesdropping.

Now, follow the link http://www.st-andrews.ac.uk/physics/quvis/ and click on the link entitled "Quantum Cryptography" under "Quantum Information". Make use of the "Step-by-step Exploration" menu of the simulation to check your answers to the questions above. If your predictions do not match the simulation outcomes, reconcile the differences between your prediction and simulation.