CSE610: Quantum Key Distribution and Communication

The *task* is for two communicating parties, "Alice" and "Bob", to possess the same long random binary string ρ without any other party knowing ρ. Once they have ρ, they can communicate messages x up to the length N of ρ with perfect secrecy via the classical **one-time pad** protocol:

- Alice sends $x' = x \oplus \rho$ to Bob.
- Bob, on receiving a string y' from Alice computes $y = y' \oplus \rho$.
- Presuming he and Alice stay "on the same page" of ρ, and that no mishaps befell the transmitted
  bits, it follows that $y = x$, so Bob can read what Alice sent.
- An eavesdropper can read x', but because ρ stays unknown and is completely random, having x' confers no information about x.

A big *cost* of this is that ρ can be used only once: if you also intercept $z' = z \oplus \rho$ then $x' \oplus z' = x \oplus \rho \oplus z \oplus \rho = x \oplus z$, so you have the difference of two well-formed plaintexts, from which much information about them can be inferred. So the one-time pad requires economical production of large numbers of random bits on demand.

A point of this to bear in mind is that the need for ρ presumes that Alice and Bob do not already have a secure channel for communication. They have only insecure channels that may be presumed no different from public reveal. The idea can work for multiple parties, which is why it is called quantum key *distribution* (QKD), but they must be told how many bits have been used by a communication involving only some of them in order to stay synchronized.

A third point is that communicating a *random* ρ is tantamount to communicating a message x. Thus the
task does not need to be immediately about communicating willful messages. It is also possible that ρ does not need to be received exactly. Plaintext messages x can be pre-processed by error-correcting codes (ECCs) as z so that damage to a moderately small proportion of bits still allows decoding x. Whether *quantum* ECCs can help with this part is getting ahead of the story. We will begin by supposing that Alice and Bob want to agree on ρ exactly.

A fourth point is that any sub-sequence of a random ρ is still random. Even if three-fourths of ρ gets wiped out, including (say) the whole first half, the leftover will still serve. This is an advantage over cases with ECCs on structured messages.

Entangle or Not?

In a perfect world, Alice would have a simple quantum solution. She would entangle pairs $|00\rangle + |11\rangle$ and send the second qubit to Bob, which they would both measure in the standard basis. By the postulates of quantum mechanics, Alice's results ρ will be perfectly random, and by entanglement, Bob will get the same results.

The zeroth problem is that willful entanglement is still relatively expensive. The first problem is that an eavesdropper, "Eve", can intercept and measure the qubits sent to Bob before sending them on.

- Her measuring them is the same to Alice as if Bob did.
- Bob will get Eve's measurement results. He could equally have gotten them himself, so he cannot tell the difference either.
- This is true even if Bob measures in a different basis from Eve.

Entanglement is indeed the basis of the second QKD proposal, by Artur Ekert of Oxford. But let's see the first, by Charles Bennett and Gilles Brassard in 1979--1984 (the **BB84** protocol).

BB84

The **nub** is that if Alice sends a qubit as $|0\rangle$ but Bob measures it as $|1\rangle$, then something affected it *en route*. What could have happened was an intermediary measuring it in the $|+\rangle, |-\rangle$ basis and getting either of those two results, whereupon Bob would have a 50-50 chance of getting $|1\rangle$ from his measurement. Likewise, if Alice sends $|+\rangle$ but Bob measures $|-\rangle$, then their privacy has been broken---though maybe by Mother Nature; i.e., not necessarily willfully.

The second "Quantum Fact" is that if the intermediary "Eve" measures in the $|0\rangle, |1\rangle$ basis, learning Alice's bit, then Bob will get the same bit but have no way to tell it has been read. Eve's measurement "collapses" what was already a basis state to the same basis state. This goes hand-in-hand with their being no bar on copying an unknown qubit value when it is known in advance to belong to a given orthonormal basis.

This raises the idea of leaving both Bob and Eve guessing as to which basis to measure in. When (a) Bob guesses right, (b) Eve guesses wrong, and (c) Eve's measurement flips the bit, Eve can be caught---if (d), this is a qubit that Bob and Alice "sacrifice" by publicly communicating their basis choices. Each of (a,b,c,d) is a potential halving of the **rate** of the protocol, meaning the proportion of valid bits of the eventual shared ρ to the total number N of qubits sent (by Alice).

Alice and Bob separately need a cost-effective way to generate truly-random bits to begin with. Each can do private measurements of qubits in the $|+\rangle$ state to get their private random strings. Tis is not part of the *task*, which is for Alice and Bob to agree on the *same* random string ρ. There are actually some non-trivial issues with getting truly-random bits that could be a separate topic, but we will presume this poses no difficulty.

Before the protocol begins, Alice and Bob agree on some matters of procedure, most particularly:

- which bits they will "sacrifice" as a test set T on which to catch Eve. The rule for T does not need to be kept secret; it can be "every odd bit of the good indices" (numbering bits from 0).
- what proportion e of errors/eavesdrops (i.e., flipped bits in T) they will tolerate. Maybe $e = 0$.

Here is the BB84 protocol:

1. Alice generates random binary strings $r \in \{0,1\}^N$ and $s \in \{|, /\}^N$.
2. For $i = 0$ to $N-1$:
   (a) if $s_i = |$ then Alice sends a qubit $\mathbf{q}_i = |0\rangle$ if $r_i = 0$; $\mathbf{q}_i = |1\rangle$ if $r_i = 1$.
   (b) if $s_i = /$ then Alice sends $\mathbf{q}_i = |+\rangle$ if $r_i = 0$ and $\mathbf{q}_i = |-\rangle$ if $r_i = 1$.
3. Bob independently generates a random string $s' \in \{|, /\}^N$ (this can be before or after Alice sends the qubits---either way, Eve cannot know s or s' at step 2).
4. For $i = 0$ to $N-1$:
   (a) if $s'_i = |$ then Bob measures $\mathbf{q}_i$ in the $|0\rangle, |1\rangle$ basis, recording $r'_i = 0$ for the outcome $|0\rangle$ and $r'_i = 1$ for the outcome $|1\rangle$.
   (b) if $s'_i = /$ then Bob measures $\mathbf{q}_i$ in the $|+\rangle, |-\rangle$ basis, recording $r'_i = 0$ for the outcome $|+\rangle$ and $r'_i = 1$ for the outcome $|-\rangle$.
5. Alice and Bob publicly reveal their strings s and s'. The set I of **good indices** are those i for which $s[i] = s'[i]$, that is, when Bob guessed to measure in the same basis Alice used.
6. Alice and Bob also reveal r_i and r'_i for $i \in I \cap T$.
7. If there are at most e indices $i \in I \cap T$ such that $r_i \neq r'_i$, then they **accept** the results. Else, they re-run the whole protocol from the start to try again.

Here is an example of a possible run and outcome---assuming no errors caused by Eve:

s	$\vert$	$\vert$	$/$	$/$	$/$	$\vert$	$\vert$	$/$	$\vert$	$/$	$/$	$\vert$
r	0	1	1	0	1	0	1	1	0	0	1	1
$\mathbf{q}$	$\vert 0\rangle$	$\vert 1\rangle$	$\vert -\rangle$	$\vert +\rangle$	$\vert -\rangle$	$\vert 0\rangle$	$\vert 1\rangle$	$\vert -\rangle$	$\vert 0\rangle$	$\vert +\rangle$	$\vert -\rangle$	$\vert 1\rangle$
Eve?												
s'	$/$	$\vert$	$\vert$	$/$	$\vert$	$\vert$	$\vert$	$/$	$/$	$/$	$/$	$\vert$
T				*			*			*		*
r'		1		0		0	1	1		0	1	1
ρ		1				0		1			1	

Alice and Bob were somewhat lucky to get a shared ρ of length 4 rather than 3 from $N = 12$. Mind you, if one of the four *ed bits in r' had been flipped, they would figure that since they have only a 1-in-4 chance of catching Eve on any one bit, then plausibly all four test bits are known to Eve, and hence would ear all bits of ρ were untrustable as well.

If Alice and Bob accept with $e = 0$, then they can be confident that there are no errors on $I \setminus T$ either. The final output ρ then is the substrings formed by the bits r_i (same as r'_i) for $i \in I \setminus T$. If they allow $e > 0$, then they can use **randomness extraction** to arrive at a shorter string ρ that is still random and with high probability reduces Eve's knowledge of ρ from e bits to nearly zero bits. (A simpler way, if they don't mind the final ρ having expected length $\Theta(N/\log N)$ rather than length proportional to N, is to apply the decoding function of a **k-error correcting code** to the good sequence, where $k = 4e|I \setminus T|$. This would subtract out Eve's expected knowledge of about k bits of the good sequence, assuming the proportion of eavesdrops on $I \setminus T$ is similar to that on $I \cap T$. The factor of 4 is because

Eve gets caught only one-fourth the time on the indices in I, when she guesses the wrong basis and the bit happens to flip. Note that I is random and unknowable to Eve at the time she could act, because it depends on how s' relates to s, and its subsequences of even and odd indices were likewise unknowable.)

Presuming success is achieved with $e = 0$ on T and $|T| = |I|/2$, the expected length of ρ is $0.25N$. The factor on N is the **rate**. This is because half the indices expect to be good, and we are sacrificing half for the test set. With smaller choices of T, rates over 27% have been reported. If $e = 1/32$ is tolerated, then the rate is knocked down to $1/8$ at most when T is half of I.

B92

This is the simplification that does away with Alice's random s and has her send $|0\rangle$ when $r_i = 0$ and $|-\rangle$ when $r_i = 1$ (or she could use $|+\rangle$ for that instead, as long as Bob knows which one she is using). Bob still has to guess which basis to measure each transmitted qubit in, and of course, what he gets depends on his choice of basis, which is according to his s' random string.

- If $s_i' = |$ and he gets $|1\rangle$, he knows that Alice could not have sent $|0\rangle$ in a clean run, so he figures Alice sent $|-\rangle$ and records $r_i' = 1$.
- If $s_i' = |$ and he gets $|0\rangle$, then a clean send could have been $|0\rangle$ or $|-\rangle$, so Bob punts.
- If $s_i' = /$ and Bob gets $|+\rangle$, then Alice could not have cleanly sent $|-\rangle$, so Bob figures it was $|0\rangle$
  and records $r_i' = 0$.
- If $s_i' = /$ and Bob gets $|-\rangle$, then it could have been $|0\rangle$ from Alice as well, so Bob punts.

Thus Bob records Alice's bit only in the 25% chance that he guesses the "wrong" basis and yet the bit still goes as Alice intended. That caps the rate at 0.25 even before we bring Eve into the picture. One good thing is that Bob's revealing the set I of indices on which he recorded bits does not give useful information to Eve in retrospect.

Unfortunately, the indices on which Bob punts cannot be used to catch Eve either. Note that Eve can never be caught if she guesses Alice sent $|0\rangle$ and uses the standard basis, or when she guesses Alice sent $|-\rangle$ and so uses the $\mathbf{X}$ basis. She will get the same as what Alice sent and not be detectable at all. So when Alice sends $|0\rangle$, the only way Eve can be caught is when she uses the $\mathbf{X}$ basis, Bob uses the standard basis, and Bob gets $|1\rangle$, which he records as $|-\rangle$ giving 1. Bob and Alice again have to sacrifice some of their good indices to see Eve's activity.

The point of the BB92 protocol is only needing two broadcast states, but it pays a penalty in rate and security---regarding the latter, it takes more test trials to catch Eve with high probability. Going the other way, there are enhancements of BB84 that use more bases, in particular, using the Pauli-$\mathbf{Y}$ basis $\left\{|i\rangle, |-i\rangle\right\}$ to boot, where $|i\rangle = |0\rangle + i|1\rangle$ and $|-i\rangle = \left(|0\rangle - i|1\rangle\right)$ (both divided by root-2, of course). These achieve somewhat higher rate and frequency of catching eavesdrops.

E91

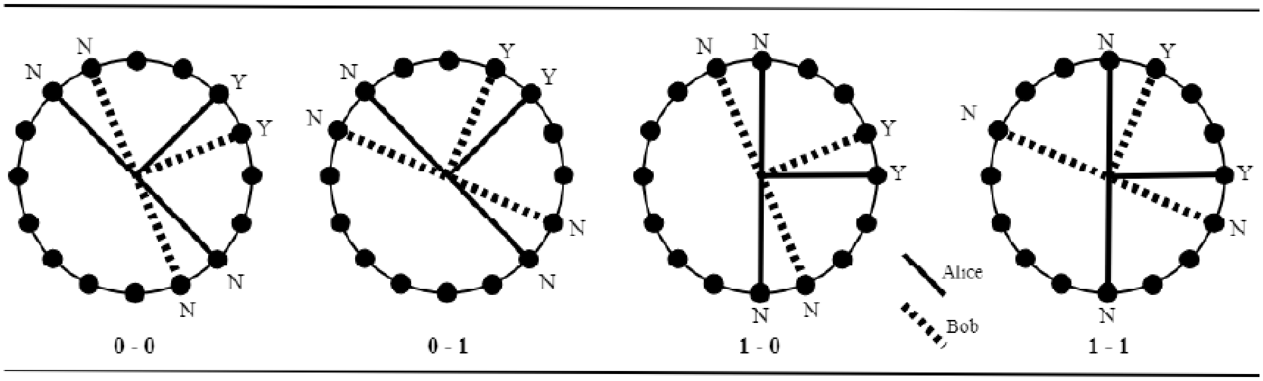
The 1991 protocol by Oxford's Artur Ekert mixes the CHSH game---where Alice and Bob always use different bases---with cases where they use the same basis. Given a pair of entangled qubits, they must use the same basis in order to guarantee that the entanglement gives them the same result on the measurement. But they need to vary their bases in order to prevent Eve from doing the same measurements.

Alice and Bob need a source of entangled qubits. One fact to note is that

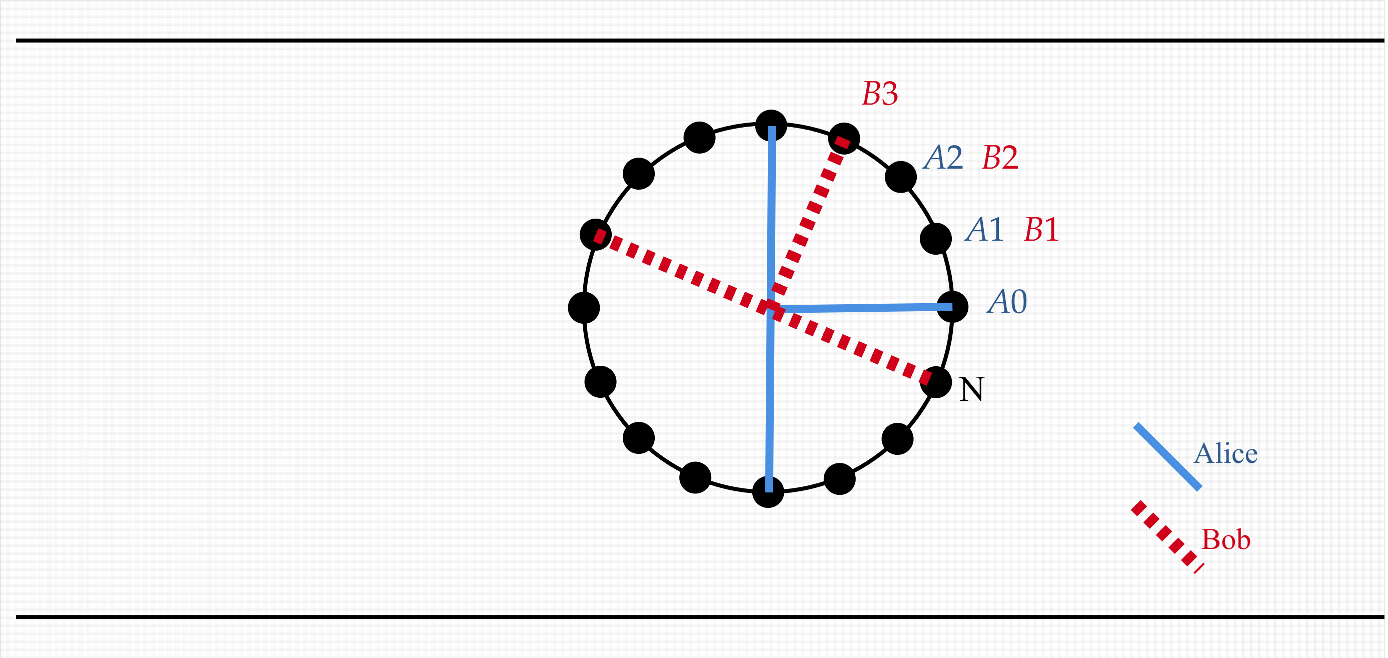
$$\frac{1}{\sqrt{2}}\left(|{++}\rangle + |{--}\rangle\right) = \frac{1}{2\sqrt{2}}\left(\begin{bmatrix}1\\1\\1\\1\end{bmatrix} + \begin{bmatrix}1\\-1\\-1\\1\end{bmatrix}\right) = \frac{1}{2\sqrt{2}}\begin{bmatrix}2\\0\\0\\2\end{bmatrix} = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right).$$

Thus it does not matter whether the source is considered to give "entangled Bell pairs" or "entangled $\mathbf{X}$ pairs"---whichever basis Alice and Bob agree on, they will get the same results. It also does not matter whether Alice knows the qubit values before Bob does: whereas a setup with "referee Ralph" was needed to close potential "loopholes" in a setting where Alice and Bob are being challenged on whether they win *fairly*, here Alice and Bob will do a cooperative analysis of cases where they don't win because Eve plays *unfairly*.

One nice feature is that the cases where Alice and Bob "punt" **are** ones where they can catch Eve. The good cases where they record bits of ρ happen only $2/9 < 1/4$ of the time, though---at least in the simple form of E91 that is invariably described. To see the design point, first recall the four possible basis choices in the CHSH game:



We can identify the basis choice with the direction of the "Y". Alice and Bob will each have three possible choices of basis rather than two, so their random strings s, s' will be ternary rather than binary. We label Alice's options $0, 1, 2$ and Bob's options $1, 2, 3$ so it is easier to tell which ones coincide. Alice chooses E, ENE, or NE; Bob ENE, NE, or NNE:



There is no separate random string r because the measurements create it. Here is the protocol in full:

1. Alice and Bob generate random strings $s \in \{0,1,2\}^N$ and $s' \in \{1,2,3\}^N$, respectively.
2. As entangled qubit pairs are sent to each in timesteps $i = 0, 1, \dots, N-1$, Alice measures hers in the basis chosen by s_i, Bob in the basis chosen by s'_i.
3. Alice and Bob then reveal s and s'. For each i:
    (a) If $s_i = s'_i = 1$ or $s_i = s'_i = 2$ then $i \in I$ and each records $r_i = 0$ if the "Y" outcome occurred, else $r_i = 1$.
    (b) If $s_i \in \{0,2\}$ and $s'_i \in \{1,3\}$ then we have a play of the CHSH game, and they put i into the test set T for further analysis.
    (c) The combination $s_i = 1, s'_i = 2$ can also be treated as a play of CHSH with the roles of Alice and Bob reversed, or just discarded. The remaining two outcomes, $s_i = 0, s'_i = 2$ and $s_i = 1, s'_i = 3$, are always discarded---for reasons similar to why different-basis cases are useless in BB84.
4. An $i \in T$ is a "win" if either $|s_i - s'_i| = 1$ and Alice and Bob got their same Y/N outcome, or $s_i = 0, s'_i = 3$, and they got opposite outcomes. They **accept** if the proportion w of wins is sufficiently close to 85%, but reject and try again if it is too close to 75%.
5. Unlike in BB84 or B92, further refinement of the recorded string r over $i \in I$ is always mandatory before the final ρ is determined.

One major immediate difference from BB84 and BB92 is that there is no notion of a perfect outcome. Even without any "Eve" or little "dents and dings" by Mother Nature of the kind discussed further below, there is random variance in their actual CHSH game outcomes. Their win percentage w can even be over 85% and yet they can't be sure that Eve didn't affect a bit or two; though they can be highly confident that Eve did not read more than a few. The only hard-and-fast conclusion is that if Eve is active *on every qubit* then w will almost certainly be below or not much higher than 75% over a large number of trials. (IMHO, sources such as these notes overstate the security.) Hence the considerations for imperfect outcomes of BB84 come into play: apply techniques from error correcting codes, hashing, and/or randomness extraction. The saving grace is the following:

> **Actions by Eve can often cause the optimal Alice-Bob strategy of the perfect CHSH game to become suboptimal even by classical standards---that is, win less than 75% of the time.**

Recall that in the matrix of the classical game, not all strategies gave 75%---some like "NNYN" gave only 25%. Incidentally, the test statistic is usually regarded as $t = 4(2w-1)$. This comes from giving $+1$ for a win and -1 for a loss, so the expectation for one play is $w \cdot (+1) \ + \ (1-w) \cdot (-1) \ = \ 2w-1$, and then the cases for the four possible Alice-Bob basis choices are added rather than averaged. Then

$w = 0.75$ gives $t = 2$ as the negative-result end, and the high end $w = \cos^2\left(\frac{\pi}{8}\right) = 0.5 + \frac{1}{2\sqrt{2}}$ conveniently makes $2w-1 = \frac{1}{\sqrt{2}}$, so that $4w = 2\sqrt{2}$. The **CHSH form** of **Bell's Inequality** states that any setting of the CHSH game that obeys local realism must give the expectation $E[t] \leq 2$.

Most sources (e.g. this and pages 41--44 of this) postulate that Eve intercepts the qubits from the source and measures each of them individually before transmitting them to Alice and Bob. She can even measure them in different bases. This gives Alice and Bob together a separable state $|\phi\rangle \otimes |\psi\rangle$. If Eve measures just one qubit, then the state will have the form $|\phi\rangle \otimes |\phi\rangle$ where $|\phi\rangle$ is one of her measurement outcomes. Alice can then measure her $|\phi\rangle$ in any basis she pleases, but there will be no effect on Bob's separated copy of $|\phi\rangle$. In any event, Eve's result places no constraint on what Bob sees even if he knows to use a basis 22.5° away from Alice's. Their measurement results are local coins, and however biased they might be, they confer no advantage in the CHSH game.

We could therefore handwave-away the analysis, but then we won't see the surprise hinted by the statement in red. If the entangled qubits initially go to Alice and she sends one to Bob, and Eve measures it first, then this is the same situation as above. The dynamically interesting order of events is:

1. Alice transmits the entangled qubit to Bob and measures hers before anyone could measure the other.
2. Eve intercepts the transmitted qubit and measures it in her basis, passing on the result to Bob.

It is possible that by a principle of time-symmetry of measurements, this is equivalent to cases above where Eve measures first. But It generates interesting analysis. The point is that Eve has the same experience as Bob in the quantum CHSH game that is free of interference, but Bob becomes a "free agent" able to measure in a different basis from Eve. The result of Alice's measurement affects Eve but not Bob.

For simplicity we suppose Eve chooses one of the bases $A0$, $A1 = B1$, $A2 = B2$, or $B3$ involved in the protocol. The analysis extends for any angle θ with similar results. Since the basis choices are all independent, we structure the analysis to fix Eve's choice and range over the options $A0, A2$ for Alice and $B1, B3$ for Bob that are in the test set T. When Alice measures first, her probabilities are 50% for

'Y', 50% for 'N' regardless of basis. We compute w as usual and t by adding the expectations of $+1$ for win, -1 for loss, over the four ways Alice and Bob can play. Put $\alpha_0 = |+\rangle$, $\alpha_1 = |-\rangle$, $\beta_0 = e^{i\pi/8}$ = ENE, $\beta_1 = e^{i5\pi/8} = \beta_0^{\perp}$, $\gamma_0 = e^{i3\pi/8}$, $\gamma_1 = e^{-i\pi/8} = \gamma_0^{\perp}$.

$Eve = A0$:

- $Alice = A0$, $Bob = B1$; agreement gives win:
  - 0.5 chance Alice gets $|0\rangle$; Eve always gets $|0\rangle$; $0.85...$ chance Bob gets $|\beta_0\rangle$ to win.
  - 0.5 chance Alice gets $|1\rangle$; Eve always gets $|1\rangle$; $0.85...$ chance Bob gets $|\beta_1\rangle$ to win.
  - Total $0.85...$, i.e., $E[w] = 0.5 + 1/\sqrt{8}$; $E[t] = 1/\sqrt{2}$.
- $Alice = A0$, $Bob = B3$; disagreement gives win:
  - 0.5 chance Alice gets $|0\rangle$, Eve always gets $|0\rangle$, $0.85...$ chance Bob gets $|\gamma_1\rangle$ to win.
  - 0.5 chance Alice gets $|1\rangle$, Eve always gets $|1\rangle$, $0.85...$ chance Bob gets $|\gamma_0\rangle$ to win.
  - in general, Alice and Eve coinciding gives the same as the CHSH expectation; $E[t] = 1/\sqrt{2}$.
- $Alice = A2$, $Bob = B1$; agreement gives win:
  - 0.5 chance Alice gets $|+\rangle$;
    - 0.5 chance Eve gets $|0\rangle$; $0.85...$ chance Bob gets $|\beta_0\rangle$ to agree with α_0.
    - 0.5 chance Eve gets $|1\rangle$; $0.15...$ chance Bob gets $|\beta_0\rangle$ to agree with α_0.
  - 0.5 chance Alice gets $|-\rangle$;
    - 0.5 chance Eve gets $|0\rangle$; $0.15...$ chance Bob gets $|\beta_1\rangle$ to agree with α_1.
    - 0.5 chance Eve gets $|1\rangle$; $0.85...$ chance Bob gets $|\beta_1\rangle$ to agree with α_1.
  - Thus this whole subcase is a 50-50 chance of win, so $E[w] = 0.5$, $E[t] = 0$.
- $Alice = A2$, $Bob = B3$; agreement gives win:
  - Once again, whether Alice gets $|+\rangle$ or $|-\rangle$, Eve is 50-50 to get $|0\rangle$ or $|1\rangle$, and those flip Bob's odds of agreement with Alice between 0.15 and 0.85, giving $E[w] = 0.5$ and $E[t] = 0$ overall.

Averaging $E[w]$ and adding up $E[t]$ across the four cases, we get the chance of a win as $\frac{1}{2} + \frac{1}{2\sqrt{8}} = 0.676776695... \ < \ 0.75$ and $E[t] = \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}} + 0 + 0 \ = \ \sqrt{2} \ < \ 2$. So Eve choosing $A0$ makes Alice and Bob fare worse than the classical bound.

$Eve = B1$:

- $Alice = A0$, $Bob = B1$; agreement gives win:
  - 0.5 chance Alice gets $|0\rangle$; $0.85...$ chance Eve gets $|\beta_0\rangle$; then Bob gets $|\beta_0\rangle$ to win.
  - 0.5 chance Alice gets $|1\rangle$; $0.85...$ chance Eve gets $|\beta_1\rangle$; then Bob gets $|\beta_1\rangle$ to win.
  - Total $0.85...$, i.e., $E[w] = 0.5 + 1/\sqrt{8}$; $E[t] = 1/\sqrt{2}$.
- $Alice = A0$, $Bob = B3$; disagreement gives win:
  - Whatever Alice's and Eve's outcome, Bob's outcome is 50-50 after Eve's measurement, so Alice and Bob are 50-50 to win: $E[w] = 0.5$, $E[t] = 0$.
- $Alice = A2$, $Bob = B1$; agreement gives win:

    - 0.5 chance Alice gets $|+\rangle$, i.e., α_0;
        - 0.85 chance Eve gets $|\beta_0\rangle$; then Bob always gets $|\beta_0\rangle$ to agree with α_0.
        - 0.15 chance Eve gets $|\beta_1\rangle$; then Bob gets $|\beta_1\rangle$ to disagree with α_0 and lose.
    - 0.5 chance Alice gets $|-\rangle$;
        - 0.15 chance Eve gets $|\beta_0\rangle$; then Bob gets $|\beta_0\rangle$ to disagree with α_1.
        - 0.85 chance Eve gets $|\beta_1\rangle$; then Bob gets $|\beta_1\rangle$ to agree with α_1.
    - Thus this whole subcase is an 85% chance of win, so $E[w] = 0.85...$, $E[t] = 1/\sqrt{2}$.
- $Alice = A2$, $Bob = B3$; agreement gives win:
    - Once again, whatever Alice's and Eve's outcome, Bob's outcome is 50-50 after Eve's measurement, so Alice and Bob are 50-50 to win: $E[w] = 0.5$, $E[t] = 0$.

Thus in this case, too, we get $E[w] \;=\; \frac{1}{2} + \frac{1}{2\sqrt{8}} = 0.676776695...$ and $E[t] = \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}} + 0 + 0 \;=\; \sqrt{2}$. The surprise is that these numbers are **less than** the values $E[w] = 0.75$ and $E[t] = 2$ from the optimal classical strategy. Thus Eve makes Alice and Bob's optimal quantum strategy become a porr classical one.

There are cases $Eve = A2$ and $Eve = B3$. How symmetrical are they with the two cases above? You can try to work out as self-study that they give the same results.

Another thing to note is that whenever Eve guesses the same basis as Alice or the same as Bob, the outcomes are the same as in the clean CHSH game. Eve is caught on the plays when she differs from both Alice and Bob. A second exercise is to see what happens if Eve chooses a basis with angle θ that
does not coincide with any of Alice and Bob's choices.

Eve or Mother Nature?

The Ekert 1991 protocol also (IMHO) affords the best situation in which to reckon the error effects covered in section 14.6 of LR chapter 14, especially depolarization. [...to write...]