# ES 274 Pset 4

Vassilios Kaxiras

December 11, 2021

**Solution** (1)**.** (i) Consider the following protocol. When Alice wants to send a bit to Bob, both her and Bob should choose, randomly and independently, whether to include their beam splitters. Then, Bob should always measure in the $\{D_2, D_1\}$ basis. After sending a stream of bits, Alice should communicate classically and openly with Bob to figure out for which bits they both had their beam splitters and for which neither of them had them. For the former, Bob will have measured exactly what Alice sent him. For the latter, Bob will have measured what Alice sent him, but bit flipped, so he should flip the bits of those parts of the messsages. Bits sent when just one of Alice or Bob had their splitters enabled should be discarded, since Bob will have measured the same results with the same probabilities regardless of what Alice sent. We can see all this by writing down the action of the system on the qubits. First, some notation: denote a photon traveling to the right (emitted from S1) as $|0\rangle$, and a photon travelling to the left (emitted from S2) as $|1\rangle$. Alice and Bob's beam splitters apply the following operation on the photon:

$$B_A = B_B = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & i \\ i & 1 \end{bmatrix} \tag{1}$$

while the mirrors between the beam splitters apply a $\sigma_x$ operation. D1 measures if the photon is in the $|1\rangle$ state, while D2 measures if the photon is in the $|0\rangle$ state. Thus we see that the four possible operations on a photon sent by Alice are

| | $\sigma_x$ | $\sigma_x B_A$ | $B_B \sigma_x$ | $B_B \sigma_x B_A$ |
|---|---|---|---|---|
| $\|0\rangle$ | $\|1\rangle$ | $\frac{1}{\sqrt{2}}(i\|0\rangle + \|1\rangle)$ | $\frac{1}{\sqrt{2}}(i\|0\rangle + \|1\rangle)$ | $i\|0\rangle$ |
| $\|1\rangle$ | $\|0\rangle$ | $\frac{1}{\sqrt{2}}(\|0\rangle + i\|1\rangle)$ | $\frac{1}{\sqrt{2}}(\|0\rangle + i\|1\rangle)$ | $i\|1\rangle$ |

As an example, suppose Alice sends the following bit stream:

$$01100001 \tag{2}$$

For each bit, denote 0 as no beam splitters, 1 as only Alice's, 2 as only Bob's, and 3 as both. Then suppose the beam splitters are chosen randomly such that

$$01302103 \tag{3}$$

Then one possibility is Bob would measure

$$10111011 \tag{4}$$

After communicating the beam splitter configuration, Bob would know to flip the first, 4th, and 7th bits he received, and discard the 2nd, 5th, and 6th bits, obtaining the message

$$0X10XX01 \tag{5}$$

which is a correct partial reconstruction of Alice's message.

(ii) In principle, this should work no matter how far Alice and Bob are. In practice, decoherence of the photon by coupling to its environment becomes more and more likely the further distance it has to travel, so if Alice and Bob are far enough away it would fail more often than not.

(iii) One-time pad works by exchanging a secret key of length at least as large as the messag being sent between the two parties. Then, the message is encrypted using that secret key, and as long as the key is kept secret, the encrypted message is cryptographically secure. Encryption works by simply adding the message to the key, mod the number of letters in your key/message alphabet. Quantum key distribution can be used to securely distribute the secret key between two parties that are physically separated, so it provides a method of safely implementing one-time pad.

(iv) Eve could intercept the message after Alice's beam splitter, apply her own beam splitter $B_1^e$ depending on the basis she wishes to measure in, and measure using two detectors $D_1^e, D_2^e$ which path the photon is on. Then, Eve can send a photon from one of two sources $S_1^e, S_2^e$ she controls through a beam splitter $B_2^e$ (if she measured with a beam splitter, otherwise she won't apply this beam splitter) to Alice. See Figure (1) for a graphical description of this setup.

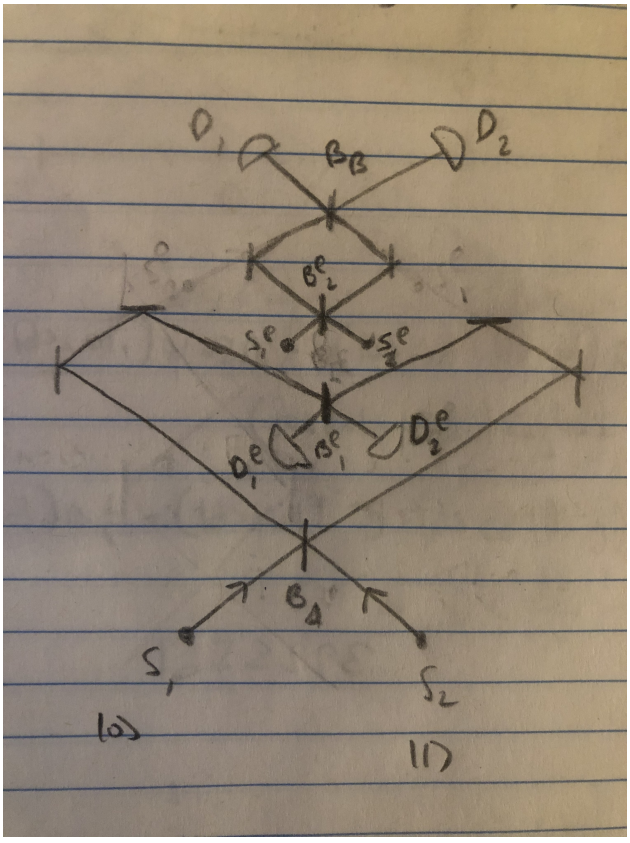


Figure 1: Eve's eavesdropping setup.

(v) Without the presence of Eve, Alice and Bob's beam splitter setup will align $\frac{1}{2}$ of the time, and bits sent when aligned will be correctly received. When the setups are not aligned, Bob will get random bits, but the classical communication step after sending the bits will lead

Bob to discard those bits and achieve an overall error rate of $\boxed{0}$.
With the presence of Eve, bits that are not discarded will correspond to bits sent with beam splitters aligned between Alice and Bob, as before. For bits where Alice and Bob both placed their beam splitters, the transmission will be perfect if Eve also places her beam splitter, while if she doesn't she will measure in the wrong basis and destroy the information, leading to a 1/2 chance of error. Similarly, for bits where Alice and Bob don't place their beam splitters, if Eve places her splitter it will lead to a 1/2 loss rate, and otherwise the transmission will be perfect. So assuming Eve places her beamsplitter randomly, the overall error rate is $\boxed{\frac{1}{4}}$.
Thus the maximum error rate acceptable for this kind of communication is $\boxed{< \frac{1}{4}}$.

(vi) Denote $X$ as the number of detections of bits on Bob's ends that are due to dark counts per second. With a resolution of $10^9$ per second, and a dark count of $10^4$ per detector, the probability that any given time slot of the $10^9$ possible slots in a detector is triggered by a dark count is $10^{-5}$. However, if either of the two detectors go off, which has a chance of $2\cdot 10^{-5}$, this will be read as a bit. Since there are $10^6$ synchronized detection slots per second, this means $E(X) = 20$. To have an error rate of at most 1/4, we need at least 60 correct bits per second. The number of correct bits measured by Bob per second is, accounting for loss factor $L$, only half of the bits having aligned bases between Alice and Bob, and the efficiency of the detectors:

$$L\frac{1}{2}10^6\frac{1}{10} = \frac{L}{2}10^5 \tag{6}$$

so we need

$$\frac{L}{2}10^5 > 60 \implies L > 0.0012 \to 29.2 \text{ dB} \tag{7}$$

so the total distance we can cover is

$$\frac{29.2}{0.2} \approx \boxed{146 \text{ km}} \tag{8}$$

**Solution** (2)**.** (i) We can see from simple geometry that

$$|H\rangle = \cos\theta|\theta\rangle - \sin\theta|\theta+\pi/2\rangle, \quad |V\rangle = \sin\theta|\theta\rangle + \cos\theta|\theta+\pi/2\rangle \tag{9}$$

So

$$\begin{aligned}\frac{1}{\sqrt{2}}(|HH\rangle + |VV\rangle) = \frac{1}{\sqrt{2}}(\cos^2\theta|\theta\theta\rangle - \cos\theta\sin\theta(|\theta\ \theta+\pi/2\rangle + |\theta+\pi/2\ \theta\rangle)+\\ \sin^2\theta|\theta+\pi/2\ \theta+\pi/2\rangle + \sin^2\theta|\theta\theta\rangle + \sin\theta\cos\theta(|\theta\ \theta+\pi/2\rangle + |\theta+\pi/2\ \theta\rangle)+\\ \cos^2\theta|\theta+\pi/2\ \theta+\pi/2\rangle) = \boxed{\frac{1}{\sqrt{2}}(|\theta\theta\rangle + |\theta+\pi/2\ \theta+\pi/2\rangle)}\end{aligned} \tag{10}$$

(ii) So, from the above we see that no matter the value of $\theta$, if we align two polarizers at angle $\theta$ to measure the two photons we will observe them to come out together along the polarization axis ($|\theta\theta\rangle$) or we will observe neither ($|\theta+\pi/2\ \theta+\pi/2\rangle$), with each outcome having probability $\frac{1}{2}$.

(iii) If the polarizers are crossed, then we will never observe any light coming through both of them, since there is no amplitude to the $|\theta\ \theta+\pi/2\rangle$, $|\theta+\pi/2\ \theta\rangle$ states. Instead, we will see a photon coming through one polarizer, with each being equally likely (probability $\boxed{\frac{1}{2}}$).

(iv) This implies that we can measure quantum correlation, or at least correlation of the type $|\Phi^+\rangle$, with rotated polarizers. If the state is not correlated, we can write it as $|\theta_1\theta_2\rangle$. Then if $\theta_1 = \theta_2$ or $\theta_1 = \theta_2 + \pi$, we can rotate the aligned polarizers from 0 to $2\pi$. When we hit $\theta_1 + \pi/2$, we will never see any photons come through, which will indicate we are not in the $|\Phi^+\rangle$ state. On the other hand, if $\theta_1 \neq \theta_2,\ \theta_1 \neq \theta_2 + \pi$, with crossed polarizers at $\theta_1, \theta_1 + \pi/2$ there will be some probability of measuring photons from both polarizers (projecting into the $|\theta_1\ \theta_1 + \pi/2\rangle$ state), in which case we will know we're not in $|\Phi^+\rangle$. So by performing these two tests we can conclude if we're in the $|\Phi^+\rangle$ state or not.

(v) We see

$$|\Phi^-\rangle = \frac{1}{\sqrt{2}}(|HH\rangle - |VV\rangle) = \frac{1}{\sqrt{2}}((\cos^2\theta - \sin^2\theta)|\theta\theta\rangle - 2\sin\theta\cos\theta(|\theta\ \theta + \pi/2\rangle + |\theta + \pi/2\ \theta\rangle) + (\sin^2\theta - \cos^2\theta)|\theta + \pi/2\ \theta + \pi/2\rangle) = \frac{1}{\sqrt{2}}(\cos(2\theta)(|\theta\theta\rangle - |\theta + \pi/2\ \theta + \pi/2\rangle) - \sin(2\theta)(|\theta\ \theta + \pi/2\rangle + |\theta + \pi/2\ \theta\rangle)) \tag{11}$$

And

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|HV\rangle + |VH\rangle) = \frac{1}{\sqrt{2}}(\sin(2\theta)(|\theta\theta\rangle - |\theta + \pi/2\ \theta + \pi/2\rangle) + \cos(2\theta)(|\theta + \pi/2\ \theta\rangle + |\theta\ \theta + \pi/2\rangle)) \tag{12}$$

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|HV\rangle - |VH\rangle) = \frac{1}{\sqrt{2}}(|\theta\ \theta + \pi/2\rangle - |\theta + \pi/2\ \theta\rangle)$$

We can make a table for the probabilities of various outcomes. Denote $x_1x_2,\ x_i \in \{0, 1\}$ as the outcome where a photon comes out of detector $i$ for the two detectors if $x_i = 1$. Then, for aligned polarizers,

| | 00 | 01 | 10 | 11 |
|---|---|---|---|---|
| $\|\Phi^+\rangle$ | $1/2$ | $0$ | $0$ | $1/2$ |
| $\|\Phi^-\rangle$ | $\cos^2(2\theta)/2$ | $\sin^2(2\theta)/2$ | $\sin^2(2\theta)/2$ | $\cos^2(2\theta)/2$ |
| $\|\Psi^+\rangle$ | $\sin^2(2\theta)/2$ | $\cos^2(2\theta)/2$ | $\cos^2(2\theta)/2$ | $\sin^2(2\theta)/2$ |
| $\|\Psi^-\rangle$ | $0$ | $1/2$ | $1/2$ | $0$ |

While for crossed polarizers,

| | 00 | 01 | 10 | 11 |
|---|---|---|---|---|
| $\|\Phi^+\rangle$ | $0$ | $1/2$ | $1/2$ | $0$ |
| $\|\Phi^-\rangle$ | $\sin^2(2\theta)/2$ | $\cos^2(2\theta)/2$ | $\cos^2(2\theta)/2$ | $\sin^2(2\theta)/2$ |
| $\|\Psi^+\rangle$ | $\cos^2(2\theta)/2$ | $\sin^2(2\theta)/2$ | $\sin^2(2\theta)/2$ | $\cos^2(2\theta)/2$ |
| $\|\Psi^-\rangle$ | $1/2$ | $0$ | $0$ | $1/2$ |

(vi) We see

$$\begin{aligned} |HH\rangle &= \cos^2\theta|\theta\theta\rangle - \cos\theta\sin\theta(|\theta\ \theta + \pi/2\rangle + |\theta + \pi/2\ \theta\rangle) + \sin^2\theta|\theta + \pi/2\ \theta + \pi/2\rangle \\ |VV\rangle &= \sin^2\theta|\theta\theta\rangle + \sin\theta\cos\theta(|\theta\ \theta + \pi/2\rangle + |\theta + \pi/2\ \theta\rangle) + \cos^2\theta|\theta + \pi/2\ \theta + \pi/2\rangle \end{aligned} \tag{13}$$

with probability $1/2$ each, we see $|HH\rangle$ or $|VV\rangle$. So we consider each case separately, and calculate the probabilities of the outcomes from two aligned polarizers:

| | 00 | 01 | 10 | 11 |
|---|---|---|---|---|
| $\|HH\rangle$ | $\sin^4\theta$ | $\cos^2\theta\sin^2\theta$ | $\cos^2\theta\sin^2\theta$ | $\cos^4\theta$ |
| $\|VV\rangle$ | $\cos^4\theta$ | $\cos^2\theta\sin^2\theta$ | $\cos^2\theta\sin^2\theta$ | $\sin^4\theta$ |

So the overall probability of the two photons coming out of both polarizers is

$$\boxed{\frac{\cos^4\theta+\sin^4\theta}{2}} \tag{14}$$

(vii) We see from the previous portion that for certain bases, we get definite results from the given classical correlation. For example, if $\theta=\pi/2$, we always see both $|VV\rangle$, or nothing. However, we do not have the quantum interference that keeps the probability of both photons leaving the polarizers at 1/2 no matter the basis. Thus we can detect that this is classical correlation by sweeping $\theta$ and observing as the rate of photon detection changes.

**Solution** (3)**.** (a) $|\Psi^-\rangle$ is the only Bell state that is antisymmetric under exchange of the two photons - all the other Bell states are symmetric. The total polarization-space wavefunction of two photons incident on a beam splitter must be symmetric, since they are bosons, so that means the space component is antisymmetric only for $|\Psi^-\rangle$ as well. Denote $|a\rangle,|b\rangle$ as the input ports of the beam splitter, and $|c\rangle,|d\rangle$ as the output ports. Then the space component of the wavefunction for $|\Psi^-\rangle$ polarized photons is

$$\frac{1}{\sqrt{2}}(|a\rangle|b\rangle-|b\rangle|a\rangle) \tag{15}$$

Under the beam splitter, this transforms to

$$\frac{1}{2\sqrt{2}}((|c\rangle+i|d\rangle)(i|c\rangle+|d\rangle)-(i|c\rangle+|d\rangle)(|c\rangle+i|d\rangle))=\frac{1}{\sqrt{2}}(|cd\rangle-|dc\rangle) \tag{16}$$

So the two photons will leave through opposite ports.
For the other Bell states, the space component is, if the photons come through both input ports,

$$\begin{aligned}\frac{1}{\sqrt{2}}(|a\rangle|b\rangle+|b\rangle|a\rangle)\rightarrow\\ \frac{1}{2\sqrt{2}}((|c\rangle+i|d\rangle)(i|c\rangle+|d\rangle)+(i|c\rangle+|d\rangle)(|c\rangle+i|d\rangle))=\frac{i}{\sqrt{2}}(|cc\rangle+|dd\rangle)\end{aligned} \tag{17}$$

So the photons will leave in the same spatial mode.

(b) Yes, you can distinguish them by applying a polarization beam splitter that only reflects light that is $|V\rangle$ polarized after each output port of the 50/50 beamsplitter. If the state is $|\Phi^\pm\rangle$, then the photons will again exit along one mode:

$$\frac{1}{2}(|HH\rangle\pm|VV\rangle)(|cc\rangle+|dd\rangle)\rightarrow\frac{1}{2}(|HHe_1e_1\rangle\pm|VVf_1f_1\rangle+|HHe_2e_2\rangle\pm|VVf_2f_2\rangle) \tag{18}$$

where $e_1,f_1$ are the outputs of the polarizing beam splitter after port $c$, while $e_2,f_2$ are the outputs of the polarizing beam splitter after port $d$.
But if the state is $|\Psi^+\rangle$, they will always exit along different ports:

$$\frac{1}{2}(|HV\rangle+|VH\rangle)(|cc\rangle+|dd\rangle)\rightarrow\frac{1}{2}(|HVe_1f_1\rangle+|VHf_1e_1\rangle+|HVe_2f_2\rangle+|VHf_2e_2\rangle) \tag{19}$$

So you can measure this with two detectors at the two output ports of the polarization beam splitter. This is graphically depicted in Figure (2).

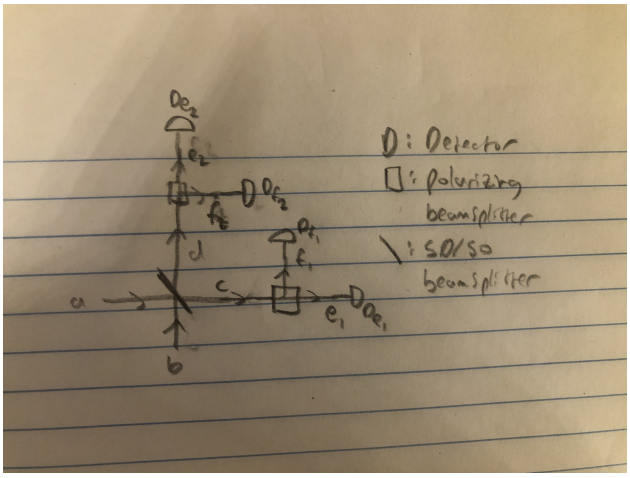


Figure 2: Setup to distinguish between $|\Phi^{\pm}\rangle$ and $|\Psi^{+}\rangle$.

(c) The initial state is (when not labelled, states are in $ABCD$ order):

$$|\psi_0\rangle = \frac{1}{\sqrt{2}}(|HV\rangle - |VH\rangle) \otimes \frac{1}{\sqrt{2}}(|HV\rangle - |VH\rangle) = \\ \frac{1}{2}(|HVHV\rangle - |VHHV\rangle - |HVVH\rangle + |VHVH\rangle) \tag{20}$$

The projection matrices for the various outcomes of the Bell measurement on BC are

$$\Pi_{\Phi^{\pm}} = (I \otimes \frac{1}{\sqrt{2}}(|HH\rangle \pm |VV\rangle) \otimes I)(I \otimes \frac{1}{\sqrt{2}}(\langle HH| \pm \langle VV|) \otimes I) = \\ \frac{1}{2}(I \otimes (|HH\rangle\langle HH| \pm |VV\rangle\langle HH| \pm |HH\rangle\langle VV| + |VV\rangle\langle VV|) \otimes I) \\ \Pi_{\Psi^{\pm}} = (I \otimes \frac{1}{\sqrt{2}}(|HV\rangle \pm |VH\rangle) \otimes I)(I \otimes \frac{1}{\sqrt{2}}(\langle HV| \pm \langle VH|) \otimes I) = \\ \frac{1}{2}(I \otimes (|HV\rangle\langle HV| \pm |VH\rangle\langle HV| \pm |HV\rangle\langle VH| + |VH\rangle\langle VH|) \otimes I) \tag{21}$$

so the outcomes after performing a Bell measurement on BC are

$$\Pi_{\Phi^{\pm}}|\psi_0\rangle = \frac{1}{4}(-|VHHV\rangle \mp |VVVV\rangle \mp |HHHH\rangle - |HVVH\rangle)_{ABCD} = \\ \frac{1}{4}(-|VVHH\rangle \mp |VVVV\rangle \mp |HHHH\rangle - |HHVV\rangle)_{DABC} = \\ \mp\frac{1}{2}\frac{1}{\sqrt{2}}(|HH\rangle \pm |VV\rangle)_{DA} \otimes \frac{1}{\sqrt{2}}(|HH\rangle \pm |VV\rangle)_{BC} \rightarrow \boxed{\mp|\Phi^{\pm}\Phi^{\pm}\rangle_{DABC}} \\ \Pi_{\Psi^{\pm}}|\psi_0\rangle = \frac{1}{4}(|VHVH\rangle \pm |VVHH\rangle \pm |HHVV\rangle + |HVHV\rangle)_{ABCD} = \\ \frac{1}{4}(|HVHV\rangle \pm |HVVH\rangle \pm |VHHV\rangle + |VHVH\rangle)_{DABC} = \\ \frac{1}{2}\frac{1}{\sqrt{2}}(|HV\rangle \pm |VH\rangle)_{DA} \otimes \frac{1}{\sqrt{2}}(|HV\rangle \pm |VH\rangle)_{BC} \rightarrow \boxed{|\Psi^{\pm}\Psi^{\pm}\rangle_{DABC}} \tag{22}$$

Thus we see that whatever state we measure for $BC$, we project $AD$ into the same state! Qualitatively, if we were to correct A, D with the appropriate Pauli matrices based on the

measurement outcome of BC, we would have teleported C to A and B to D and AD would be in the $|\Psi^-\rangle$ state.

(d) Let's consider all the cases. Denote $|\psi_1\rangle$ as the state after we measure A, D, which we perform before measuring BC in the Bell basis. There are 4 outcomes for A,D, each with 2 possible measurement outcomes for B, C afterwards:

$$\begin{aligned}
|\psi_1\rangle = |HVHV\rangle &\implies \Pi_{\Phi^\pm}|\psi_1\rangle \to 0 \\
|\psi_1\rangle = |HVHV\rangle &\implies \Pi_{\Psi^\pm}|\psi_1\rangle \to |H\rangle\frac{1}{\sqrt{2}}(|VH\rangle \pm |HV\rangle)|V\rangle = \pm|H\Psi^\pm V\rangle \\
|\psi_1\rangle = |VHHV\rangle &\implies \Pi_{\Phi^\pm}|\psi_1\rangle \to |V\rangle\frac{1}{\sqrt{2}}(|HH\rangle \pm |VV\rangle)|V\rangle = |V\Phi^\pm V\rangle \\
|\psi_1\rangle = |VHHV\rangle &\implies \Pi_{\Psi^\pm}|\psi_1\rangle \to 0 \\
|\psi_1\rangle = |HVVH\rangle &\implies \Pi_{\Phi^\pm}|\psi_1\rangle \to |V\rangle\frac{1}{\sqrt{2}}(\pm|HH\rangle + |VV\rangle)|V\rangle = \pm|H\Phi^\pm H\rangle \\
|\psi_1\rangle = |HVVH\rangle &\implies \Pi_{\Psi^\pm}|\psi_1\rangle \to 0 \\
|\psi_1\rangle = |VHVH\rangle &\implies \Pi_{\Phi^\pm}|\psi_1\rangle \to 0 \\
|\psi_1\rangle = |VHVH\rangle &\implies \Pi_{\Psi^\pm}|\psi_1\rangle \to |V\rangle\frac{1}{\sqrt{2}}(|HV\rangle \pm |VH\rangle)|H\rangle = |V\Psi^\pm H\rangle
\end{aligned} \tag{23}$$

If we were instead to measure A, D after the Bell basis measurement, we can consider the 4 different starting dual Bell states and the resulting states after measuring A, D at the end:

$$\begin{aligned}
|\Phi^\pm\Phi^\pm\rangle_{DABC} &\to |H\Phi^\pm H\rangle_{ABCD} \text{ or } |V\Phi^\pm V\rangle_{ABCD} \\
|\Psi^\pm\Psi^\pm\rangle_{DABC} &\to |H\Psi^\pm V\rangle_{ABCD} \text{ or } |V\Phi^\pm H\rangle_{ABCD}
\end{aligned} \tag{24}$$

This is exactly the same as the results when we measured A, D first! Furthermore, all the probabilities are also the same (all 1/8). So, it appears that the time-ordering of quantum measurements is not unique, and it doesn't matter at what point you make your measurement, but rather what the measurement is.