1. Imperfect BB84 with mismatched basis alignment

We let $|\alpha\rangle = \cos\alpha\,|0\rangle + \sin\alpha\,|1\rangle$, $|\alpha_\perp\rangle = -\sin\alpha\,|0\rangle + \cos\alpha\,|1\rangle$, and $H = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$ the Hadamard matrix. Alice and Bob use the BB84 protocol to generate a one-time pad, *but they do not know that their respective encoding and decoding basis are misaligned by a (small) angle* α. We remind the first steps of the protocol:

- Alice generates two independent random bit sequences x_i and e_i, $i = 1, \dots, n$. Each sequence is i.i.d with uniform probabilities $1/2$ for each bit. If $e_i = 0$ she sends (to Bob) a qubit in state $|x_i\rangle$. If $e_i = 1$ she sends a qubit in state $H\,|x_i\rangle$.
- Bob generates a random sequence $d_1 \dots d_N$ of i.i.d bits with uniform probabilities $1/2$. If $d_i = 0$ Bob measures the received state with the basis $|\alpha\rangle$, $|\alpha_\perp\rangle$, and if $d = 1$ he measures with the basis $H\,|\alpha\rangle$, $H\,|\alpha_\perp\rangle$. When measurements output $|\alpha\rangle$ or $H\,|\alpha\rangle$ he registers $y_i = 0$, and when measurements output $|\alpha_\perp\rangle$ or $H\,|\alpha_\perp\rangle$ he registers $y_i = 1$.

(a) Compute $\mathbb{P}(x_i = y_i | e_i = d_i = 0, x_i = 0)$; $\mathbb{P}(x_i = y_i | e_i = d_i = 0, x_i = 1)$; and $\mathbb{P}(x_i = y_i | e_i = d_i = 1, x_i = 0)$; $\mathbb{P}(x_i = y_i | e_i = d_i = 1, x_i = 1)$. Deduce $\mathbb{P}(x_i = y_i | e_i = d_i)$

(b) Explain the rest of the protocol and in particular explain how Alice and Bob can evaluate the misalignment of their basis thanks to the security test (assuming for some reason they know the protocol is noiseless and there is no eavesdropper).

2. Imperfect dense coding with an unknown entangled state

Alice and Bob use dense coding to communicate 2 classical bits. *But they dont know they share state* $|S\rangle = \frac{1}{\sqrt{3}}(|0\rangle_A \otimes |0\rangle_B + |1\rangle_A \otimes |1\rangle_B + |0\rangle_A \otimes |1\rangle_B)$ *instead of the usual Bell state.* We recall the steps used by Alice and Bob:

- In order to send message $ij \in \{00, 01, 10, 11\}$ Alice applies the unitary $Z_A^i X_A^j$ to her qubit and then sends it to Bob. We recall $X = \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$ and $Z = \begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}$.
- Once in possession of the pair Bob performs a measurement in the Bell basis $|\Psi^\pm\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle$, $|\Phi^\pm\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle$. Bob's decoding map is $|\Psi^+\rangle \to 00$, $|\Phi^+\rangle \to 01$, $|\Psi^-\rangle \to 10$, $|\Phi^-\rangle \to 11$.

(a) Prove that $|S\rangle$ is an *entangled* state.

(b) For each message ij, what is the state of the pair of qubits in Bob's lab *just after* receiving Alice's qubit?

(c) Suppose now Alice intends to send message 10. What are the possible measurement outcomes of Bob and their respective probabilities?

(d) Still assuming Alice's message is 10, what is the probability of a transmission error?

3. QKD: a scheme between three parties with W states

Notation: In this problem it is more convenient to use the following notations. The computational basis states $|0\rangle$, $|1\rangle$ (or Z basis) are called $|z_+\rangle$, $|z_-\rangle$ and the states $|\pm\rangle = \frac{1}{2}(|0\rangle \pm |1\rangle$ (or X basis) are denoted $|x_+\rangle$ and $|x_-\rangle$. Note that these states are the outcomes of measurements of the observables X and Z (Pauli matrices).

Suppose three parties A, B, C share a number of $|W\rangle$ states,

$$|W\rangle = \frac{1}{\sqrt{3}}(|z_+ z_- z_-\rangle + |z_- z_+ z_-\rangle + |z_- z_- z_+\rangle)$$

One can show that this is a fully entangled state in the sense that it is not equal a product state of the type $A \otimes B \otimes C$ nor of the type $(AB) \otimes C$, $(AC) \otimes B$, $(BC) \otimes A$.

The goal of A, B, C is to generate pairs of secret keys or "one-time pads" (one for AB, one for BC, one for AC) by making appropriate local measurements and using classical communication. Consider the following protocol for each instant of time $t = 1, \ldots N$:

1. A, B, C each choose an X or Z basis at random. Thus they have 8 choices $i - j - k$ with $i, j, k \in \{X, Z\}$. They perform a local measurement and keep the outcome secret.

2. They announce publicly their choice of basis.

3. They keep their measurement outcomes (secret) if the choice of basis are $Z - X - X$, $X - Z - X$, $X - X - Z$. The rest of the outcomes are discarded.

4. For the above choices only one of them choose the Z basis. At each such instant he is called the "decider". The decider looks at his measurement outcome and (here suppose the decider is C):

   - if it is $|z_+\rangle$ he announces publicly to A and B to discard their measurement outcomes.
   - if it is $|z_-\rangle$ he announces publicly to A and B to keep their measurement outcomes and turn them into their key bits: $|x_+\rangle \to 1$ and $|x_-\rangle \to 0$. One can show that the key bits of A and B are equal.

   When the decider is A (resp. B) she instructs BC (resp. AC) publicly similarly.

5. A, B, C do a security test similar to BB84 by revealing a small fraction of their secret bits. If the test passes they keep their secret pairwise keys. If it fails they abort communication.

Question a: Check that the W-state can be written as

$$|W\rangle = \sqrt{\frac{2}{3}}|z_-\rangle_A \otimes \frac{|x_+x_+\rangle_{BC} - |x_-x_-\rangle_{BC}}{\sqrt{2}} + \frac{1}{\sqrt{3}}|z_+\rangle_A \otimes \frac{|x_+\rangle_B - |x_-\rangle_B}{\sqrt{2}} \otimes \frac{|x_+\rangle_C - |x_-\rangle_C}{\sqrt{2}}$$

Deduce that for the three basis choices $Z-X-X$, $X-Z-X$, $X-X-Z$ the possible outcomes of measurements are given by this table (the decider has the Z basis and the two other parties the X basis). Compute also the probabilities for each outcome.

Alice	Bob	Charlie	Decider
z_-	x_-	x_-	
z_-	x_+	x_+	Alice
z_+	x_- or x_+	x_- or x_+	
x_-	z_-	x_-	
x_+	z_-	x_+	Bob
x_- or x_+	z_+	x_- or x_+	
x_-	x_-	z_-	
x_+	x_+	z_-	Charlie
x_- or x_+	x_- or x_+	z_+	

Question b: Convince yourself that each pair of parties has its own one-time pad. What is then the length of each one-time pad (i.e., what fraction of N) ? On average, to produce one secret-key bit, how many quantum bits are needed in this protocol?

4. Entanglement Concentration and Dilution Protocols

We study two related 'Local Operation and Classical Communication' (LOCC) protocols. Alice and Bob are at two distant locations and are allowed to perform *local operations* (unitaries and measurements) and also communicate through *classical messages*.

I. Entanglement concentration: Alice and Bob share a Bell pair $|\Phi\rangle_{AB} = \frac{1}{\sqrt{2}}(|00\rangle_{AB} + |11\rangle_{AB})$. Their task is to transform it to $|\Psi_\theta\rangle = \cos\theta|00\rangle_{AB} + \sin\theta|11\rangle_{AB}$, $0 < \theta < 2\pi$. Alice also has an extra ancilla qubit. We guide you through the LOCC:

1. The extra ancilla qubit of Alice is in the state $|0\rangle_{A'}$ and she performs a local unitary on AA':

$$U = F_{0A} \otimes 1_{A'} + iF_{1A} \otimes X_{A'}$$

where

$$F_{0A} = \begin{pmatrix} \cos\theta & 0 \\ 0 & \sin\theta \end{pmatrix}, \quad F_{1A} = \begin{pmatrix} \sin\theta & 0 \\ 0 & \cos\theta \end{pmatrix}, \quad 1_{A'} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad X_{A'} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Compute the final *global state* of Alice and Bob (for the three qubits ABA').
Hint: the initial state can be written $|\Phi\rangle_{AB} \otimes |0\rangle_{A'} = \frac{1}{\sqrt{2}}(|0\rangle_A \otimes |0\rangle_{A'} \otimes |0\rangle_B + |1\rangle_A \otimes |0\rangle_{A'} \otimes |1\rangle_B)$.

2. Alice then does a measurement of her *ancilla* qubit in the computational basis $\{|0\rangle_{A'}, |1\rangle_{A'}\}$. Suppose the outcome for A' is $|i\rangle_{A'}$, $i \in \{0, 1\}$. What are the possible outcome *global states* for each $i = 0, 1$ and their respective probabilities p_0, p_1 ?

3. Finally Alice transmits to Bob one classical bit $i \in \{0, 1\}$ corresponding to her outcome. Propose simple *local unitaries* that Alice and Bob must perform in order to succeed with their task. What is the overall success probability for this protocol ?

II. Entanglement dilution: This is a reverse task. Alice and Bob now initially share the pair $|\Psi_\theta\rangle = \cos\theta|00\rangle_{AB} + \sin\theta|11\rangle_{AB}$, $0 < \theta < 2\pi$. They should transform it to a pure Bell state $|\Phi\rangle_{AB} = \frac{1}{\sqrt{2}}(|00\rangle_{AB} + |11\rangle_{AB})$. Alice can use an ancilla qubit again. We guide you through the LOCC:

4. Alice performs the same local unitary U on her two qubits AA'. Her ancilla qubit is initially in the satte $|0\rangle_{A'}$ as before. Compute the final *global state* of the three qubits ABA'.

5. Alice then measures her *ancilla* qubit in the basis $\{|0\rangle_{A'}, |1\rangle_{A'}\}$. Explain what are the possible outputs for the *global state* (of ABA') and their corresponding probabilities.

6. Finally Alice sends a classical bit to Bob to inform him about the outcome of her measurement. And now, what can they both conclude about the success probability of this protocol?

Solution to Problem 1:

(a)

- For $e_i = 0$ Alice sends qubits $|x_i\rangle = |0\rangle, |1\rangle$. And for $d_i = 0$ Bob's measurement basis is $|\alpha\rangle, |\alpha_\perp\rangle$. Thus applying Born's rule:

$$P(x_i = y_i | e_i = d_i = 0, x_i = 0) = |\langle\alpha|0\rangle|^2 = (\cos\alpha)^2$$
$$P(x_i = y_i | e_i = d_i = 0, x_i = 1) = |\langle\alpha_\perp|1\rangle|^2 = (\cos\alpha)^2$$

- Similarly, for $e_i = 1$ Alice sends qubits $H|x_i\rangle = |+\rangle, |-\rangle$. And for $d_i = 1$ Bob's measurement basis is $H|\alpha\rangle, H|\alpha_\perp\rangle$. Thus applying Born's rule:

$$P(x_i = y_i | e_i = d_i = 1, x_i = 0) = |\langle\alpha| H^\dagger H |0\rangle|^2 = (\cos\alpha)^2$$
$$P(x_i = y_i | e_i = d_i = 1, x_i = 1) = |\langle\alpha_\perp| H^\dagger H |1\rangle|^2 = (\cos\alpha)^2$$

Therefore since $P(x_i = 0) = P(x_i = 1) = 1/2$

$$P(x_i = y_i | e_i = d_i = 0) = \frac{1}{2}(\cos\alpha)^2 + \frac{1}{2}(\cos\alpha)^2 = (\cos\alpha)^2$$

and

$$P(x_i = y_i | e_i = d_i = 1) = \frac{1}{2}(\cos\alpha)^2 + \frac{1}{2}(\cos\alpha)^2 = (\cos\alpha)^2$$

Finally,

$$P(x_i = y_i | e_i = d_i) = P(x_i = y_i | e_i = d_i, e_i = 0)P(e_i = 0) + P(x_i = y_i | e_i = d_i, e_i = 1)P(e_i = 1)$$
$$= \frac{1}{2}(\cos\alpha)^2 + \frac{1}{2}(\cos\alpha)^2 = (\cos\alpha)^2$$

We check that when $\alpha = 0$ this probability is one (ideal BB84). Other sanity checks are for $\alpha = \pi/2$ this prob is zero and for $\alpha = \pi/4$ this prob is $1/2$ (should be intuitive).

(b) Once the quantum communication and measurement phases are finished, Alice and Bob reveal on a public channel their basis choices e_i and d_i. Each time $e_i \neq d_i$ they discard bits x_i and y_i. The set P of other bits forms their one-time pad. They check agreement $x_i = y_i$ with security test: they reveal on a public channel a small fraction of bits in P and (assuming the protocol is noiseless and there is no eavesdropper) the fraction of tested bits which agree is $(\cos\alpha)^2 \approx 1 - \alpha^2/2$ (for α small). From this fraction they get an estimate of α.

Solution to problem 2:

(a) Proof by contradiction: suppose $|S\rangle$ is not entangled:

$$|S\rangle = \big(a|0\rangle + b|1\rangle\big) \otimes \big(c|0\rangle + d|1\rangle\big) = ac|00\rangle + ad|01\rangle + bc|10\rangle + bd|11\rangle .$$

Then $ac = ad = bd = \frac{1}{\sqrt{3}}$ and $bc = 0$. This implies $b \neq 0$ since $bd \neq 0$; and $c = 0$ since $b \neq 0$ and $bc = 0$. But then $ac = 0$ and since we also have $ac = \frac{1}{3}$ we find a contradiction. In conclusion $|S\rangle$ must be entangled.

(b) Here are the states in Bob's lab once he receives Alice's qubit:

- Alice's message 00: Bob gets $|S\rangle = \frac{1}{\sqrt{3}}\big(\,|00\rangle + |11\rangle + |01\rangle\,\big)$
- Alice's message 01: Bob gets $X\,|S\rangle = \frac{1}{\sqrt{3}}\big(\,|10\rangle + |01\rangle + |11\rangle\,\big)$
- Alice's message 10: Bob gets $Z\,|S\rangle = \frac{1}{\sqrt{3}}\big(\,|00\rangle - |11\rangle + |01\rangle\,\big)$
- Alice's message 11: Bob gets $ZX\,|S\rangle = \frac{1}{\sqrt{3}}\big(\,-|10\rangle + |01\rangle - |11\rangle\,\big)$

(c) Alice sends 10 so Bob possesses the pair

$$Z\,|S\rangle = \frac{1}{\sqrt{3}}\big(\,|00\rangle - |11\rangle + |01\rangle\,\big).$$

The measurement outcomes and probabilities for Bob are

- $|\Psi^+\rangle$ with probability $|\,\langle\Psi^+|\,Z\,|S\rangle\,|^2 = \frac{1}{2}\cdot\frac{1}{3}(1-1)^2 = 0$
- $|\Psi^-\rangle$ with probability $|\,\langle\Psi^-|\,Z\,|S\rangle\,|^2 = \frac{1}{2}\cdot\frac{1}{3}(1+1)^2 = \frac{2}{3}$
- $|\Phi^+\rangle$ with probability $|\,\langle\Phi^+|\,Z\,|S\rangle\,|^2 = \frac{1}{2}\cdot\frac{1}{3}(1)^2 = \frac{1}{6}$
- $|\Phi^-\rangle$ with probability $|\,\langle\Phi^-|\,Z\,|S\rangle\,|^2 = \frac{1}{2}\cdot\frac{1}{3}(1)^2 = \frac{1}{6}$

Note that probabilities indeed sum to one.

(d) According to the decoding map of Bob:

$$P(\text{transmission error}) = P(\text{Bob doesnt get } \Psi^-) = 0 + \frac{1}{6} + \frac{1}{6} = \frac{1}{3}$$

Solution to Problem 3:

Question a: Firstly, one can check that:

$$\frac{1}{\sqrt{2}}\left(|x_+\rangle - |x_-\rangle\right) = |z_-\rangle \implies \frac{1}{\sqrt{2}}\left(|x_+\rangle - |x_-\rangle\right) \otimes \frac{1}{\sqrt{2}}\left(|x_+\rangle - |x_-\rangle\right) = |z_-z_-\rangle \tag{1}$$

and:

$$|x_\pm x_\pm\rangle = \frac{1}{\sqrt{2}}(|z_+\rangle \pm |z_-\rangle) \otimes \frac{1}{\sqrt{2}}(|z_+\rangle \pm |z_-\rangle) \tag{2}$$

$$= \frac{1}{2}(|z_+z_+\rangle + |z_-z_-\rangle \pm |z_+z_-\rangle \pm |z_-z_+\rangle) \tag{3}$$

So:

$$\frac{1}{\sqrt{2}}(|x_+x_+\rangle - |x_-x_-\rangle) = \frac{1}{\sqrt{2}}(|z_+z_-\rangle + |z_-z_+\rangle) \tag{4}$$

Therefore:

$$|W\rangle = \frac{1}{\sqrt{3}}\left(|z_-\rangle \otimes (|z_+z_-\rangle + |z_-z_+\rangle) + |z_+\rangle \otimes |z_-z_-\rangle\right) \tag{5}$$

$$= \frac{1}{\sqrt{3}}\left(|z_-\rangle \otimes (|x_+x_+\rangle - |x_-x_-\rangle) + |z_+\rangle \otimes \frac{1}{\sqrt{2}}(|x_+\rangle - |x_-\rangle) \otimes \frac{1}{\sqrt{2}}(|x_+\rangle - |x_-\rangle)\right) \tag{6}$$

Assume the basis is $Z - X - X$, we get:

$$P(|z_+\rangle_A) = \langle W|\left(|z_+\rangle_A \langle z_+|_A \otimes I_B \otimes I_c\right)|W\rangle = \frac{1}{3} \tag{7}$$

1. Conditional on the outcome $|z_+\rangle_A$ (which happens with probability $\frac{1}{3}$), Bob and Charlie obtain an outcome in the set $\{|x_+x_+\rangle, |x_-x_+\rangle, |x_+x_-\rangle, |x_-x_-\rangle\}$ with uniform probability ($\frac{1}{4}$)

2. Conditional on the outcome $|z_-\rangle_A$ (which happens with probability $\frac{2}{3}$), Bob and Charlie get either $|x_-x_-\rangle_{BC}$ with probability $\frac{1}{2}$ or $|x_+x_+\rangle_{BC}$ with probability $\frac{1}{2}$.

Question b: Let's compute for instance the probability that Charlie and Bob get the same one-time-pad:

1. First of all, there are 3 interesting basis among $2^3 = 8$ possible basis, so $\frac{3}{8}$ chances to have a correct basis.

2. Conditional on the previous event, Alice is chosen as the decider with probability $\frac{1}{3}$

3. Conditional on the previous events, Alice measures the outcome $|z_-\rangle$ with probability $\frac{2}{3}$

Therefore, in total, the probability to generate a common key-bit between Charlie and Bob is $\frac{3}{8}\frac{1}{3}\frac{2}{3} = \frac{1}{12}$ for each shared W state (so 3 qubits shared). Thus with 36 qubits BC generate 1 key-bit, but at the same time also AB and AC have generated 1 key-bit each (when the third person was a decider). Thus with 36 qubits the trio generates 3 key bits (associated to the couples AB,, BC, AC). On average this protocol consumes 12 qubits to generate one key bit.

Remark: In the Ekert-91 protocol (see the book Nielsen and Chuang for example) there are 9 basis choices out of which 2 are good to generate a common key-bit between the two parties A and B. So for 9 EPR pairs, i.e., 18 qubits we have 2 key-bits. On average the Ekert-91 protocol consumes 9 qubits to generate 1 key-bit.

Solution to Problem 4:

1) We find

$$U|0\rangle_A \otimes |0\rangle_{A'} = \cos\theta|0\rangle_A \otimes |0\rangle_{A'} + i\sin\theta|0\rangle_A \otimes |1\rangle_{A'}$$

and

$$U|0\rangle_A \otimes |1\rangle_{A'} = \sin\theta|1\rangle_A \otimes |0\rangle_{A'} + i\cos\theta|1\rangle_A \otimes |1\rangle_{A'}$$

From which we deduce the final global state:

$$\frac{1}{\sqrt{2}}(\cos\theta|00\rangle_{AB} + \sin\theta|11\rangle_{AB}) \otimes |0\rangle_{A'} + \frac{1}{\sqrt{2}}(\sin\theta|00\rangle_{AB} + \cos\theta|11\rangle_{AB}) \otimes |1\rangle_{A'}$$

2) Alice does a measurement on A'. The possible resulting states are

$$\frac{1}{\sqrt{2}}(\cos\theta|00\rangle_{AB} + \sin\theta|11\rangle_{AB}), \qquad \frac{1}{\sqrt{2}}(\sin\theta|00\rangle_{AB} + \cos\theta|11\rangle_{AB}) \otimes |1\rangle_{A'}$$

with probabilities

$$p_0 = \frac{1}{2}(\cos^2\theta + \sin^2\theta) = \frac{1}{2}, \qquad p_1 = \frac{1}{2}(\cos^2\theta + \sin^2\theta) = \frac{1}{2}$$

3) When Bob reeives the classical bit 0 or 1, he knows what is the resulting global state. If 0 is the outcome then Alice and Bob aplly the local unitaries $1_A \otimes 1_B$. If 1 is the outcome then Alice and Bob aplly the local unitaries $X_A \otimes X_B$.
The success probability of the protocol is always $1/2 + 1/2 = 1$.
Remark: this protocol is a simple example of so called 'entanglement concentration'.

4) We compute:

$$\begin{aligned}
&U|\Psi_\theta\rangle \otimes |0\rangle_{A'} \\
&= \cos^2\theta|0\rangle_A|0\rangle_{A'}|0\rangle_B + i\cos\theta\sin\theta|0\rangle_A|1\rangle_{A'}|0\rangle_B + \sin^2\theta|1\rangle_A|0\rangle_{A'}|1\rangle_B + i\sin\theta\cos\theta|1\rangle_A|1\rangle_{A'}|1\rangle_B \\
&= (\cos^2\theta|00\rangle_{AB} + \sin^2\theta|11\rangle_{AB}) \otimes |0\rangle_{A'} + i\sin\theta\cos\theta(|00\rangle_{AB} + |11\rangle_{AB}) \otimes |1\rangle_{A'}
\end{aligned}$$

5) Alice Measures her ancilla qubit. The possible outcome states are

$$\frac{(\cos^2\theta|00\rangle_{AB} + \sin^2\theta|11\rangle_{AB})}{\sqrt{\cos^4\theta + \sin^4\theta}} \otimes |0\rangle_{A'}, \qquad \frac{1}{\sqrt{2}}(|00\rangle_{AB} + |11\rangle_{AB}) \otimes |1\rangle_{A'}$$

with probabilities

$$p_0 = \cos^4\theta + \sin^4\theta, \qquad p_1 = 2(\sin\theta\cos\theta)^2$$

6) Alice send s a classical bit 0 or 1 to Bob according to her measurement result. Hence they both know what is the resulting state. The success probability of the protocol is thus

$$p_1 = 2(\sin\theta\cos\theta)^2$$

Remark: this protocol is an example of 'entanglement dilution'.

We see that entanglement concentration and dilution do not have symmetric success probabilities.