# Lecture Notes

## edX Quantum Cryptography: Week 3

# Contents

We have seen in Week 1 an example of communication between Alice and Bob, where the transmitted message is hidden from any eavesdropper Eve. There, we have seen the importance of using a large key $K$ shared between Alice and Bob, but looks completely random from Eve's perspective. In the next few lectures, we will concern ourselves with how to establish such a key.

In this week, we will first learn about ways to quantify quantum information, which will be crucial in formulating what does it mean to be secure in cryptographic protocols.

## 3.1 When are two quantum states almost the same?

It will be important for us to have some notion of what it means to approximately produce a particular quantum state.

### 3.1.1 Trace distance

One measure of closeness that is of extreme importance in quantum cryptography, and also in the design of quantum circuits is the trace distance. Let us suppose, we would like to implement a protocol or algorithm that produces state $\rho_{\text{ideal}}$. Unfortunately, due to imperfections, our protocol produces the state $\rho_{\text{real}}$. If we now use this protocol or algorithm as a subroutine in a much larger protocol or computation, how is this larger protocol affected if we can only make $\rho_{\text{real}}$ instead of $\rho_{\text{ideal}}$?

Intuitively, it is clear that if $\rho_{\text{real}}$ and $\rho_{\text{ideal}}$ are nearly impossible to distinguish, then it should not matter much in the large protocol which one we use. We would thus like a distance measure that is directly related to how well we can distinguish the two states. To this end, let us suppose that we really don't know whether we have the real or ideal state. Imagine that we are given $\rho_{\text{real}}$ and $\rho_{\text{ideal}}$ each with probability $1/2$, and we are challenged to distinguish them. To this end, we can perform a measurement using some operators $M_{\text{real}}$ and $M_{\text{ideal}} = \mathbb{I} - M_{\text{real}}$. The probability of distinguishing the two states is then

$$p_{\text{succ}} = \frac{1}{2}\operatorname{tr}[M_{\text{real}}\rho_{\text{real}}] + \frac{1}{2}\operatorname{tr}[M_{\text{ideal}}\rho_{\text{ideal}}] = \frac{1}{2} + \frac{1}{2}\operatorname{tr}[M_{\text{real}}(\rho_{\text{real}} - \rho_{\text{ideal}})] \ . \tag{3.1}$$

To find the best measurement, we can optimize the term $M_{\text{real}}$ above over all measurement operators. We know (see Week 1 lecture notes, section on POVMs) that $0 \leq M_{\text{real}} \leq \mathbb{I}$, i.e. $M_{\text{real}}$'s eigenvalues all lie between 0 and 1. Thus the maximum success probability is given by

$$p_{\text{succ}}^{\max} = \frac{1}{2} + \frac{1}{2}\max_{0\leq M\leq \mathbb{I}} \operatorname{tr}[M(\rho_{\text{real}} - \rho_{\text{ideal}})] \ . \tag{3.2}$$

What is, then, the operator $M$ that would maximize the trace quantity $\operatorname{tr}[M(\rho_{\text{real}} - \rho_{\text{ideal}})]$? This question has been analyzed in [Hel76], and the optimal $M$ is the projector onto the positive eigenspace of $\rho_{\text{real}} - \rho_{\text{ideal}}$. More concretely, consider the diagonalized form of the linear operator $\rho_{\text{real}} - \rho_{\text{ideal}}$, and denote this diagonal matrix as $D = \sum_i d_i |d_i\rangle\langle d_i|$. Furthermore, denote the set $S_+ = \{j | d_j > 0\}$. The optimal $M$ is then given by

$$M_{\text{opt}} = \sum_{j\in S_+} |d_j\rangle\langle d_j|. \tag{3.3}$$

It turns out the the trace distance precisely captures this idea of distinguishing states.

**Definition 3.1.1 — Trace distance.** The *trace distance* between two quantum states $\rho_{\text{real}}$ and $\rho_{\text{ideal}}$ is given by

$$D(\rho_{\text{real}}, \rho_{\text{ideal}}) = \max_{0\leq M\leq \mathbb{I}} \operatorname{tr}[M(\rho_{\text{real}} - \rho_{\text{ideal}})] \ . \tag{3.4}$$

The trace distance can also be written as

$$D(\rho_{\text{real}}, \rho_{\text{ideal}}) = \frac{1}{2}\operatorname{tr}\left[\sqrt{A^\dagger A}\right] , \tag{3.5}$$

where $A = \rho_{\text{real}} - \rho_{\text{ideal}}$.

In the literature, you will also see the trace distance written using the following notation

$$D(\rho_{\text{real}}, \rho_{\text{ideal}}) = \frac{1}{2}\|\rho_{\text{real}} - \rho_{\text{ideal}}\|_{\text{tr}} = \frac{1}{2}\|\rho_{\text{real}} - \rho_{\text{ideal}}\|_{1} . \tag{3.6}$$

If two states are close in trace distance, then there exists no measurement - no process in the universe - that can tell them apart very well. It also means that if we use a subroutine that makes $\rho_{\text{real}}$ instead of $\rho_{\text{ideal}}$ and the two are close in trace distance, then we can safely conclude that also the surrounding larger protocol cannot see much difference. Otherwise, we could use the large protocol to tell the two states apart, but we know this cannot be.

**Definition 3.1.2 — Closeness in terms of trace distance.** Two quantum states $\rho$ and $\sigma$ are $\varepsilon$-close, if $D(\rho,\sigma) \leq \varepsilon$. We also write this as $\rho \approx_\varepsilon \sigma$.

**Proposition 3.1.1** The trace distance is a metric, that is, a proper distance measure that corresponds to our intuitive notions of distance. We have the following properties for all states $\rho, \sigma, \tau$:

1. Non-negative: $D(\rho,\sigma) \geq 0$, where equality is achieved if and only if $\rho = \sigma$.
2. Symmetric: $D(\rho,\sigma) = D(\sigma,\rho)$.
3. Triangle inequality: $D(\rho,\sigma) \leq D(\rho,\tau) + D(\tau,\sigma)$.
4. Convexity: $D(\sum_i p_i\rho_i, \sigma) \leq \sum_i p_i D(\rho_i,\sigma)$.

■ **Example 3.1.1** Consider $\rho_1 = |0\rangle\langle 0|$ and $\rho_2 = |+\rangle\langle +|$. Firstly, calculate

$$\rho_1 - \rho_2 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} - \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix}. \tag{3.7}$$

Therefore, the trace distance is equal to

$$D(\rho_1,\rho_2) = \frac{1}{2}\cdot\frac{1}{2}\operatorname{tr}\sqrt{\begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix}^2} = \frac{1}{2}\cdot\frac{1}{2}\operatorname{tr}\sqrt{\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}} = \frac{1}{\sqrt{2}}. \tag{3.8}$$

Another way to do so is to first consider the diagonalization of $\rho_1 - \rho_2$, which can be done by first calculating its eigenvalues, solving the following equation:

$$\det\begin{pmatrix} \frac{1}{2} - \lambda & -\frac{1}{2} \\ -\frac{1}{2} & -\frac{1}{2} - \lambda \end{pmatrix} = 0. \tag{3.9}$$

The solutions are given by $\lambda = \pm\frac{1}{\sqrt{2}}$. One can also find the eigenvector $|e_+\rangle = (x \quad y)^T$ corresponding to $\lambda = \frac{1}{\sqrt{2}}$,

$$\frac{1}{2}\begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} x \\ y \end{pmatrix} \quad\Longrightarrow\quad \frac{x}{y} = \frac{-1}{\sqrt{2}-1}. \tag{3.10}$$

On the other hand, normalization condition gives $x^2 + y^2 = 1$, and the solution is found to be

$$x = \cos\frac{\pi}{8}, \quad y = \sin\frac{\pi}{8}. \tag{3.11}$$

The optimal measurement operator that distinguishes $\rho_1, \rho_2$ is then given by $M_{\text{opt}} = |e_+\rangle\langle e_+|$, while

$$\operatorname{tr}\left[M_{\text{opt}}(\rho_1 - \rho_2)\right] = \frac{1}{\sqrt{2}}. \tag{3.12}$$

■

Since states which are $\varepsilon-$close to each other cannot be distinguished well, it will later be helpful to have the notion of a set of states which are all $\varepsilon-$close to a particular state $\rho$. This is often called the $\varepsilon-$ball of $\rho$.

**Definition 3.1.3 — $\varepsilon-$ball of $\rho$.** Given any density matrix $\rho$, the *$\varepsilon-$ball of $\rho$* is defined as the set of all states $\rho'$ which are $\varepsilon-$close to $\rho$ in terms of trace distance, i.e.

$$\mathscr{B}^{\varepsilon}(\rho) := \{\rho' \mid \rho' \geq 0, \mathrm{tr}(\rho') = 1, D(\rho,\rho') \leq \varepsilon\}. \tag{3.13}$$

### 3.1.2 Fidelity

Although we have not seen this in the lectures, there is another common measure for closeness of states is known as the fidelity, which for pure states is directly related to their inner product.

**Definition 3.1.4 — Fidelity.** Given density matrices $\rho_1$ and $\rho_2$, the *fidelity* between $\rho_1$ and $\rho_2$ is

$$F(\rho_1,\rho_2) = \mathrm{tr}\left[\sqrt{\sqrt{\rho_1}\rho_2\sqrt{\rho_1}}\right] . \tag{3.14}$$

For pure states $\rho_1 = |\Psi_1\rangle\langle\Psi_1|$ and $\rho_2 = |\Psi_2\rangle\langle\Psi_2|$ the fidelity takes on a simplified form:

$$F(\rho_1,\rho_2) = |\langle\Psi_1|\Psi_2\rangle| . \tag{3.15}$$

If only one of the states $\rho_1 = |\Psi_1\rangle\langle\Psi_1|$ is pure, we have

$$F(\rho_1,\rho_2) = \sqrt{\langle\Psi_1|\rho_2|\Psi_1\rangle} . \tag{3.16}$$

Although the fidelity is not a metric (since $F(\rho_1,\rho_2) = 0$ does not imply that $\rho_1 = \rho_2$), it does have an intuitive interpretation, if we were to verify whether we managed to produce a desired target state $|\Psi\rangle$. Suppose that we want to build a machine that produces $|\Psi\rangle\langle\Psi|$, yet we are only able to produce some state $\rho$. Let us suppose we now measure $\rho$ to check for success. We can do this (theoretically) by measuring

$$M_{\mathrm{succ}} = |\Psi\rangle\langle\Psi| , \tag{3.17}$$
$$M_{\mathrm{fail}} = \mathbb{I} - |\Psi\rangle\langle\Psi| . \tag{3.18}$$

The success probability is directly related to the fidelity between the true output $\rho$ and the target state $|\Psi\rangle$ as

$$\mathrm{tr}[M_{\mathrm{succ}}\rho] = \langle\Psi|\rho|\Psi\rangle = F(|\Psi\rangle,\rho)^2 . \tag{3.19}$$

It is interesting to note that another way to write the fidelity is as

$$\max_{|\rho_{AP}\rangle,|\sigma_{AP}\rangle} |\langle\rho_{AP}|\sigma_{AP}\rangle| , \tag{3.20}$$

where $|\rho_{AP}\rangle$ and $|\sigma_{AP}\rangle$ are purifications of the states $\rho_A$ and $\sigma_A$ using a purifying system $P$.

**Proposition 3.1.2** For any two quantum states $\rho,\sigma$, the fidelity satisfies the following properties

1. Between 0 and 1: $0 \leq F(\rho,\sigma) \leq 1$.
2. Symmetric: $F(\rho,\sigma) = F(\sigma,\rho)$.
3. Multiplicative under tensor product: $F(\rho_1 \otimes \rho_2, \sigma_1 \otimes \sigma_2) = F(\rho_1,\sigma_1) \cdot F(\rho_2,\sigma_2)$.
4. Invariant under unitary operations: $F(\rho,\sigma) = F(U\rho U^{\dagger}, U\sigma U^{\dagger})$.
5. Relation to trace distance: $1 - F(\rho,\sigma) \leq D(\rho,\sigma) \leq \sqrt{1-F^2(\rho,\sigma)}$. Conversely, we also have that $1-D(\rho,\sigma) \leq F(\rho,\sigma) \leq \sqrt{1-D^2(\rho,\sigma)}$. This is known as the Fuchs-van de Graaf inequality [FV99].

## 3.2 Measuring uncertainty: the min-entropy

In many quantum protocols, we will be measuring quantum states and not get a key immediately. Instead, we will create a cq-state

$$\rho_{XE} = \sum_{x\in\{0,1\}^n} p_x|x\rangle\langle x|_X \otimes \rho_x^E \ , \tag{3.21}$$

where we have used the shorthand $p_x = \text{Prob}(X = x)$, and $p_x$ is not uniform. Of course, we could consider the distance of this state to an ideal state $\rho_{XE}^{\text{ideal}}$, but it will typically be extremely large. Nevertheless, we could ask how useful the state $\rho_{XE}$ for obtaining a key, for example, by performing some computation on the string $X$. This motivates us to try and find a measure of uncertainty about the classical string $X$.

### 3.2.1 The min-entropy

Let us first consider just the state

$$\rho_X = \sum_x p_x|x\rangle\langle x|_X \ . \tag{3.22}$$

Note that this means that we are effectively considering the probability distribution $p_x$ over strings $x$. How could we measure the uncertainty inherent in $\rho_X$? When talking about communication, one very important measure is the von Neumann or Shannon entropy $H(X) = -\sum_x p_x \log p_x$. Is this quantity also a useful measure in the context of cryptography?

To think about this question, let us consider the following scenario: Suppose we have purchased a box (possibly from Eve!) which generates a string $x = x_1,\ldots,x_n$. If the string was uniformly random, then $p_x = 1/2^n$ and $H(X) = n$. If $x$ is uncorrelated from Eve, then we could hope to use the string $x$ as an encryption key for use in the one-time pad. Suppose now that while we are promised that $x$ is uncorrelated from Eve, the distribution $p_x$ is *not* uniform. However, we are guaranteed that the entropy is still $H(X) \approx n/2$, and $n$ is very large. We know nothing else about the box. Would you still be willing to use $x$ as an encryption key?

On first sight, the situation may not be so bad. After all, while the string does not have maximum entropy $H(X) = n$, it still has half as much entropy, which for very large $n$ is after all still extremely large. Intuitively, this should mean that there is a lot of uncertainty for Eve, or does it?

Let us consider the following distribution:

$$p_x = \begin{cases} \frac{1}{2} & \text{for } x = 11\ldots 1 \\ \frac{1}{2}\cdot\frac{1}{2^n-1} & \text{otherwise .} \end{cases} \tag{3.23}$$

**Exercise 3.2.1** Show that the entropy for this distribution is $H(X) \approx n/2$. ■

But is there a lot of uncertainty for Eve? Note that the probability that the box generates the string $x = 11\ldots 1$ is $1/2$, independent of the length of the string! This means that whenever we use $x$ as an ecryption key, Eve will be able to guess the key, and thus decrypt the message with probability $1/2$. Eve's probability of guessing is extremely large, even when we send a very large message.

We thus see that the von Neumann/Shannon entropy is not a good measure for cryptography. However, there exists an alternate entropy which is indeed useful for such purposes.

**Definition 3.2.1 — Min-entropy.** Given any probability distribution $\{p_x\}_x$, the *min-entropy* $\mathrm{H}_{\min}$ is defined as $\mathrm{H}_{\min}(X) = \mathrm{H}_{\min}(\rho_X) = -\log\max_x p_x$ .

In our example above, we see that $\mathrm{H}_{\min}(X) = -\log 1/2 = 1$. That is, the min-entropy is constant! Note that the min-entropy precisely captures our intuitve idea of what it means for Eve to be uncertain about $x$: Eve could guess the string with probability $1/2$. In general, we would all guess the most likely string, and the probability that we are correct is precisely $P_{\text{guess}}(X) = \max_x p_x$. The min-entropy thus has as very neat operational interpretation as

$$\mathrm{H}_{\min}(X) = -\log P_{\text{guess}}(X) \ . \tag{3.24}$$

R We may wonder why this was not also the right measure of uncertainty in the communication tasks we considered. Note that there we have always look at the case where we have states of the form $\rho^{\otimes n}$ where $n$ is reasonably large. Following Shannon's line of thought and thinking of $i(x) := -\log p_x$ as the surprisal, that is, the information gained when we observe $x$, the Shannon entropy measured the *average* surprisal $H(X) = \sum_x p_x i(x)$. When doing cryptography, however, we are always interested in the worst case, not the average case. The min-entropy $\mathrm{H}_{\min}(X) = \min_x i(x)$ is precisely this smallest surprisal. Fig.3.1 shows the difference between these quantities, for a binary random variable.

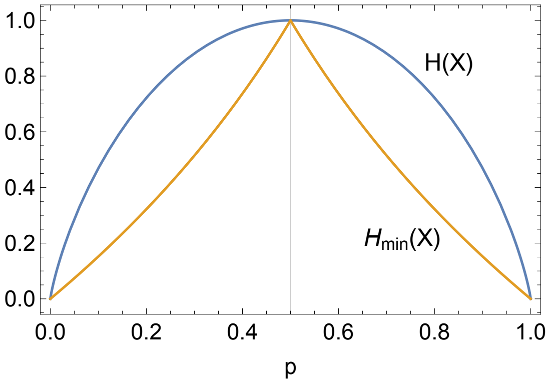

Figure 3.1: For a binary random variable $X = \{0,1\}$, the comparison between Shannon entropy $H(X)$ and its min-entropy $\mathrm{H}_{\min}(X)$.

**Exercise 3.2.2** Show that the min-entropy satisfies the following bounds:

$$0 \leq \mathrm{H}_{\min}(X) \leq H(X) \leq \log|X|. \tag{3.25}$$

■

### 3.2.2 The conditional min-entropy

Can we also quantify the uncertainty about $X$ *given* some extra quantum register $E$? It turns out that just like for the von Neumann entropy, the min-entropy has a conditional variant $\mathrm{H}_{\min}(X|E)$ developed in [Ren08]. The easiest way to think about the conditional min-entropy is in terms of the probability that Eve manages to guess $X$ given access to her quantum register $E$. Note that we see from the cq-state in Eq. (3.21) that Eve has state $\rho_x^E$ with probability $p_x$ and her goal is to guess $x$ by making a measurement on $E$. This is precisely the problem of distinguishing quantum states that we considered earlier.

**Definition 3.2.2 — Conditional min-entropy.** Consider a bipartite cq-state $\rho_{XE}$ where $X$ is classical. The *conditional min-entropy* $\mathrm{H}_{\min}(X|E)$ can be written as

$$\mathrm{H}_{\min}(X|E)_{\rho_{XE}} := -\log P_{\text{guess}}(X|E) \ , \tag{3.26}$$

where $P_{\text{guess}}(X|E)$ is the probability that Eve guesses $x$, maximized over all possible measurements

$$P_{\text{guess}}(X|E) := \max_{\{M_x\}_x} \sum_x p_x \operatorname{tr}\left[M_x \rho_x^E\right] \;, \tag{3.27}$$

where the maximization is taken over all POVMS $\{M_x \geq 0 \mid \sum_x M_x = \mathbb{I}\}$. In this context, $E$ is also called *side information* about $X$. When it is clear from context, we omit the subscript $\rho_{XE}$, i.e. we write $\mathrm{H}_{\min}(X|E)_{\rho_{XE}} = \mathrm{H}_{\min}(X|E)$.

How could we ever hope to compute this quantity? When $x \in \{0,1\}$ takes on only two values, then it is easy to find the optimal measurement, and the guessing probability $P_{\text{guess}}$ is directly related to the distinguishability of reduced states $\rho_0^E$ and $\rho_1^E$, i.e. the trace distance $D(\rho_0^E, \rho_1^E)$. We shall see this in the following example.

■ **Example 3.2.1** Consider the state $\rho_{XE} = \frac{1}{2}|0\rangle\langle 0|_X \otimes |0\rangle\langle 0|_E + \frac{1}{2}|1\rangle\langle 1|_X \otimes |+\rangle\langle +|_E$. Then the conditional min-entropy $\mathrm{H}_{\min}(X|E) = -\log P_{\text{guess}}(X|E)$ where

$$\begin{aligned}
P_{\text{guess}}(X|E) &= \max_{\substack{M_1, M_2 \geq 0 \\ M_1 + M_2 = \mathbb{I}}} \left[\frac{1}{2}\operatorname{tr}(M_0|0\rangle\langle 0|_E) + \frac{1}{2}\operatorname{tr}(M_1|+\rangle\langle +|_E)\right] && (3.28)\\
&= \max_{0 \leq M \leq \mathbb{I}} \left[\frac{1}{2}\operatorname{tr}(M|0\rangle\langle 0|_E) + \frac{1}{2}\operatorname{tr}(|+\rangle\langle +|_E) - \frac{1}{2}\operatorname{tr}(M|+\rangle\langle +|_E)\right] && (3.29)\\
&= \frac{1}{2} + \frac{1}{2} \max_{0 \leq M \leq \mathbb{I}} \operatorname{tr}[M(|0\rangle\langle 0|_E - |+\rangle\langle +|_E)] && (3.30)\\
&= \frac{1}{2} + \frac{1}{2}\, D(|0\rangle\langle 0|_E, |+\rangle\langle +|_E). && (3.31)
\end{aligned}$$

■

However, if $x$ can take more than two possible values, then it is in general difficult to compute $P_{\text{guess}}(X|E)$ by hand. Nevertheless, finding the optimal success probability is a so-called semi-definite program (SDP) and can be evaluate efficiently (in the dimension of the states $\rho_x^E$) using for example Matlab or Julia.

For any cq-state $\rho_{XE}$ we have

$$0 \leq \mathrm{H}_{\min}(X|E) \leq \log|X| \;. \tag{3.32}$$

Note that the assumption that $X$ is classical here is important: in particular, $\mathrm{H}_{\min}(X|E)$ can be negative if $X$ is a genuine quantum register. Furthermore, we have

$$\mathrm{H}_{\min}(X|E) \geq \mathrm{H}_{\min}(X) - \log|E| \;. \tag{3.33}$$

### A general quantum conditional min-entropy

In the fully general case, the system $X$ as we have seen above is not necessarily classical, but can also be quantum (to make explicitly this difference, we use $A$ to label such a quantum system). How should the conditional min-entropy $\mathrm{H}_{\min}(A|E)$ look like? To gain some intuition on how such a quantity should be defined, think of the guessing probability as a way of quantifying how close one may get *classically maximally correlated* with the classical system $X$, i.e. by guessing it correctly. Therefore, a quantum extension of this concept would be to, when only allowing to perform operations upon $E$, get as close as possible to the maximally entangled state between $A$ and $E$.

**Definition 3.2.3 — Quantum conditional min-entropy, (KRS09).** Given any bipartite density matrix $\rho_{AE}$, with $A$ having dimension $|A|$, the conditional min-entropy is

$$\mathrm{H}_{\min}(A|E) := -\log\left[|A| \cdot \mathrm{Dec}(A|E)\right], \tag{3.34}$$

$$\mathrm{Dec}(A|E) := \max_{\Lambda_{E\to A'}} F((\mathbb{I}_A \otimes \Lambda_{E\to A'})\rho_{AE}, |\Phi\rangle\langle\Phi|_{AA'})^2, \tag{3.35}$$

where $|\Phi\rangle_{AA'} := \frac{1}{\sqrt{|A|}}\sum_{i=1}^{|A|} |a_i\rangle_A \otimes |a_i\rangle_{A'}$ is the maximally entangled state between $A$ and $A'$, and the maximization is performed over all quantum channels $\Lambda$ mapping system $E$ to $A'$. The function $F$ is the fidelity that we have seen in Def. 3.1.4.

An alternative way to express the conditional min-entropy is

$$\mathrm{H}_{\min}(A|E) := \max_{\sigma_B} \sup\{\lambda \in \mathbb{R} | \rho_{AB} \leq 2^{-\lambda}\mathbb{I}_A \otimes \sigma_B\}. \tag{3.36}$$

### Smoothed min-entropy

As one has seen earlier in the discussion on trace distance, due to imperfections in a protocol or algorithm we often do not excactly produce the state $\rho_{XE}$ that we want, rather, we can only manage to produce a state which is close, $\rho'_{XE}$, and we do not know the form of $\rho'_{XE}$ (other than the fact that it is $\varepsilon-$close to $\rho_{XE}$). For this reason, it is usually more physically relevant to look at the *smoothed min-entropy*, which gives us the maximum value of $\mathrm{H}_{\min}(X|E)$ over all states $\rho'_{AE} \in \mathscr{B}^{\varepsilon}(\rho_{AE})$.

**Definition 3.2.4 — Smoothed conditional min-entropy.** Consider a bipartite cq-state $\rho_{XE}$ where $X$ is classical. The *smoothed conditional min-entropy* $\mathrm{H}^{\varepsilon}_{\min}(X|E)$ can be written as

$$\mathrm{H}^{\varepsilon}_{\min}(X|E)_{\rho} := \max_{\rho' \in \mathscr{B}^{\varepsilon}(\rho)} \mathrm{H}_{\min}(X|E)_{\rho'}. \tag{3.37}$$

## 3.3 What it means to be ignorant

Before establishing keys, let us be precise about what we actually want to achieve. We have already sketched before that we desire the keys to be picked from a uniformly random distribution, and Eve to be uncorrelated. Classically, we could say that this should mean that the probability of selecting any $n$-bit key $k$ is $\mathrm{Prob}(K = k) = p(k) = 1/2^n$, and the key $k$ is independent of some classical information, denoted by $e$, that the eavesdropper may have gathered. That is, $p(k) = p(k|e)$.

Clearly, it makes no sense to talk about some probability distribution over classical keys $k$ conditioned on classical strings $e$ in the quantum case. After all, Eve may have gathered quantum information about the key! That is, the state between the register holding the key, let us call it $K$, and the register of Eve, let us call it $E$, is a cq-state

$$\rho_{KE} = \sum_k p_k |k\rangle\langle k| \otimes \rho_k^E\ . \tag{3.38}$$

This implies that depending on the key $k$, Eve has a quantum state $\rho_k^E$ that she may measure to gain some information about the key. Ideally, the fact that Eve knows nothing can be expressed in the following definition, which we refer to as ignorance about the key.

To motivate the definition of ignorance, let us first consider a few examples, where for simplicity we consider just a single bit of key. Our examples can however be easily extended to arbitrary many keys, and you're encouraged to check.

■ **Example 3.3.1** First, let us consider the state

$$\rho_{KE} = \frac{1}{2}\sum_{k\in\{0,1\}} |k\rangle\langle k|_K \otimes |k\rangle\langle k|_E\ . \tag{3.39}$$

Clearly, we have $\rho_K = \mathrm{tr}_E\left(\rho_{KE}\right) = \mathbb{I}_K/2$. That is the key is uniform. But clearly Eve knows everything about the key: whenever $K$ is in the state $|k\rangle\langle k|$, then so is $E$! You may see the information that Eve has as simply a classical piece of paper that has an exact copy of $k$. States of the form above are also called classically maximally correlated states. Both systems are diagonal in the standard basis, and the both systems are prepared precisely in the same state $|k\rangle\langle k|$ with some probability. ■

■ **Example 3.3.2** Let us now consider the state $\rho_{KE} = |0\rangle\langle 0|_K \otimes \rho_E$. It sure appears Eve is uncorrelated. However, $\rho_K$ is certainly not uniform. In fact, the only possible key is $k = 0$, so it is indeed easy to guess the key for anyone. ■

■ **Example 3.3.3** Consider the maximally entangled state

$$\rho_{KE} = |\Psi\rangle\langle\Psi|_{KE}$$

between $K$ and $E$, that is, $|\Psi\rangle_{KE} = \left(|0\rangle_K|0\rangle_E + |1\rangle_K|1\rangle_E\right)/\sqrt{2}$. As you have calculated before, we have $\rho_K = \mathrm{tr}_E\left(\rho_{KE}\right) = \mathbb{I}/2$. That is, the key $X$ is uniform. But is it uncorrelated? Clearly not, no matter what basis we measure $K$ in, there always exists a corresponding measurement on $E$ that yields the same outcome. This is because for all unitaries $U$, we have

$$\begin{aligned}
U_K \otimes U_E^*|\Psi\rangle_{KE} &= (U_K \otimes \mathbb{I}_E)(\mathbb{I}_K \otimes U_E^*)|\Psi\rangle_{KE} && (3.40)\\
&= (U_K \otimes \mathbb{I}_E)((U_K^*)^T \otimes \mathbb{I}_E)|\Psi\rangle_{KE} && (3.41)\\
&= (U_K \otimes \mathbb{I}_E)(U_K^\dagger \otimes \mathbb{I}_E)|\Psi\rangle_{KE} && (3.42)\\
&= (U_K U_K^\dagger \otimes \mathbb{I}_E)|\Psi\rangle_{KE} && (3.43)\\
&= |\Psi\rangle_{KE}, && (3.44)
\end{aligned}$$

where in the second equality, we have made used of a special property that holds for $|\Psi\rangle_{KE}$: for any $U$, $(\mathbb{I}_K \otimes U_E)|\Psi\rangle_{KE} = (U_K^T \otimes \mathbb{I}_E)|\Psi\rangle_{KE}$. Therefore, the corresponding measurement on $E$ is simply to measure in the basis defined by $U_E^*$ (i.e. the basis in which $U_E^*$ is diagonalized). ■

Therefore, we conclude that an eavesdropper Eve is ignorant of a key if and only if the following conditions hold.

**Definition 3.3.1 — Ignorant.** Consider the joint cq-state $\rho_{KE}$ of an $n$-bit key $K$ and the eavesdropper Eve, $E$. Eve is *ignorant* about the key $K$ if and only if

$$\rho_{KE} = \frac{1}{2^n}\mathbb{I}_K \otimes \rho_E. \tag{3.45}$$

That is, the key is uniform *and* uncorrelated from Eve.

In any actual implementation, we can never hope to attain the perfection as given by the state in Eq. (3.45). However, we can hope to get close to such an ideal state, motivating the following definition.

**Definition 3.3.2 — Almost ignorant.** Consider the joint cq-state $\rho_{KE}^{\mathrm{real}}$ of an $n$-bit key $K$ and the eavesdropper Eve, $E$. Eve is *almost ignorant* about the key $K$ if and only if

$$D\left(\rho_{KE}^{\mathrm{real}}, \rho_{KE}^{\mathrm{ideal}}\right) \leq \varepsilon\,, \tag{3.46}$$

where $\rho_{KE}^{\mathrm{ideal}} = \frac{1}{2^n}\mathbb{I}_K \otimes \rho_E$.

Why would this be a good definition? Recall that the trace distance measures exactly how well we can distinguish two scenarios. We saw that if two states are $\varepsilon$-close in trace distance, then no measurement can tell them apart with an advantage more than $\varepsilon/2$, i.e. if we were given one of the two states with equal probability, *any measurement* allowed by quantum mechanics would only tell them apart with probability $1/2+\varepsilon/2$. This is an advantage of at most $\varepsilon/2$ over a random guess, which would be correct with probability $1/2$.

This has important consequences if we want to later use the key in another protocol, for example, in an an encryption protocol like the one-time pad. Recall from Week 2 lecture notes that an encryption scheme is secret/secure if and only if for all prior distributions over the messages $p(m)$, and for all messages $m$, we should have $p(m)=p(m|c)$, where $c$ denotes the ciphertext. Such a secrecy can be achieved using the one-time pad, if Eve is completely ignorant about the key. You may think of the one-time pad scheme as a type of measurement to distinguish $\rho_{KE}^{\text{ideal}}$ and $\rho_{KE}^{\text{real}}$. If this protocol would behave very differently if we use the $\rho_{KE}^{\text{real}}$ instead of the ideal $\rho_{KE}^{\text{ideal}}$, then this would give us a means to distinguish the two states very well. But this is precisely ruled out if the states are close in trace distance!

In conclusion, if $D\left(\rho_{KE}^{\text{real}},\rho_{KE}^{\text{ideal}}\right)\leq\varepsilon$, while $\rho_{KE}^{\text{ideal}}$ leads to the probabilty distribution $p(m)=p(m|c)$, then we should also have that when using the real state $\rho_{KE}^{\text{real}}$, $p(m)\approx_{\varepsilon}p(m|c)$ should hold. This means that in the analysis of any subsequent protocol we can assume that we have the ideal key, at the expense of only a very small error $\varepsilon$.

## 3.4 Uncertainty principles: a bipartite guessing game

In this section, we first see how to construct a simple guessing game that allows us to prove security against an eavesdropper Eve who can prepare quantum states, but who otherwise stores and processes only classical information. The crucial property of quantum mechanics which allows us to make this security proof is called the *uncertainty principle*. Such a principle tells us how well Eve can or cannot predict the outcomes of two incompatible measurements on Alice's state.

As a warmup, let us first consider the case where Eve only has classical memory. That is, she might make measurements on the qubits during the transmission, but she cannot keep any entanglement herself. This is effectively equivalent to Eve actually preparing Alice's qubits herself, and can be analyzed in the form of a guessing game defined below:

**Definition 3.4.1 — Guessing game - Alice and Eve.** Suppose Alice and Eve play the following game:

1. Eve prepares a qubit $\rho_A$ and sends it to Alice.
2. Alice chooses a random bit $\Theta\in\{0,1\}$.
3. If $\Theta=0$, then Alice measures $\rho_A$ in the standard basis; if $\Theta=1$, then she measures in the Hadamard basis.
4. Alice obtains and records a measurement outcome $X\in\{0,1\}$.
5. Alice announces $\Theta$.
6. Eve wins if she can guess the bit $X$.

How may we make sure that Eve cannot fully predict Alice's measurement outcome $X$? As a simple example, let us return to Example 3.3.2 where the joint state between Alice and Eve is

$$\rho_{AE}=|0\rangle\langle 0|_A\otimes\rho_E, \tag{3.47}$$

where Alice measures system $A$ either in the standard or Hadamard basis in order to obtain the key $K$. If Alice measures in the standard basis, Eve can always predict the outcome perfectly. However, if Alice measures in the Hadamard basis, Eve can only make a random guess, since by measuring Alice obtains outcome $|+\rangle$ and $|-\rangle$ each with probability $\frac{1}{2}$!

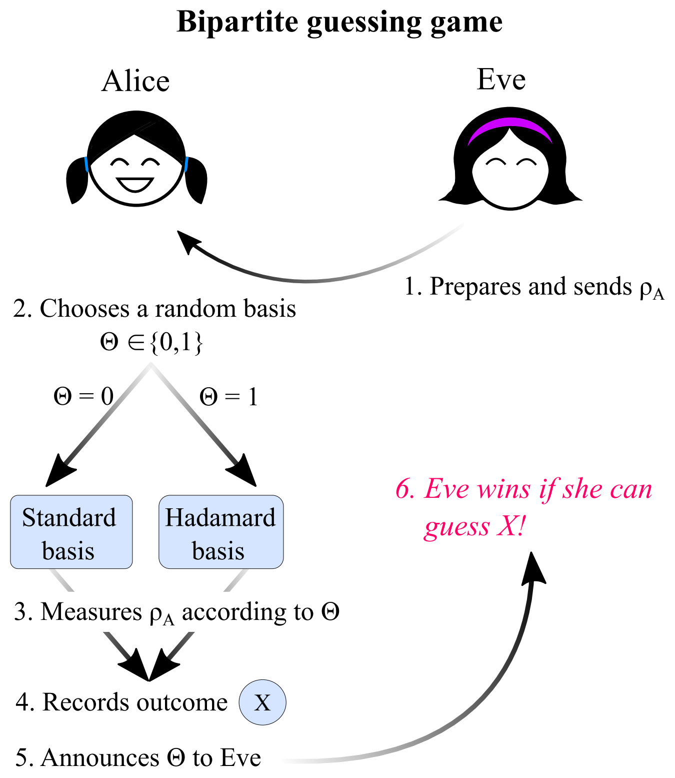
Bipartite guessing game
Alice
Eve
1. Prepares and sends ρ_A
2. Chooses a random basis Θ ∈{0,1}
Θ = 0
Θ = 1
Standard basis
Hadamard basis
3. Measures ρ_A according to Θ
4. Records outcome
X
5. Announces Θ to Eve
6. Eve wins if she can guess X!

Figure 3.2: The guessing game between Alice and Eve, where Eve prepares a quantum state and sends it to Alice, who choses randomly to measure in the standard basis or in the Hadamard basis. Eve then tries to guess Alice's measurement outcome, given the basis she chosen.

To see why this captures the essence of the uncertainty principle, note that if the measurements are incompatible, then there exists no state $\rho_A$ that Eve can prepare, that would allow her to guess the outcomes for both choices of measurements with certainty. Uncertainty can thus be quantified by a bound on the average probability that Eve correctly guesses $X$:

$$P_{\text{guess}}(X|\Theta) = p(\Theta = 0) \cdot P_{\text{guess}}(X|\Theta = 0) + p(\Theta = 1) \cdot P_{\text{guess}}(X|\Theta = 1) \tag{3.48}$$

$$= \frac{1}{2} \cdot \left[P_{\text{guess}}(X|\Theta = 0) + P_{\text{guess}}(X|\Theta = 1)\right] \leq c, \tag{3.49}$$

where the second equality holds if Alice chooses her measurement basis $\Theta$ at random, namely with uniform probability $\frac{1}{2}$ for each option. In the case where Eve holds no additional information except for the basis where Alice has performed the measurement, the quantity $c$ can be shown to be strictly less than 1.

To see why this is the case, suppose that Eve aims to correctly guess $X$ all of the time. In particular, she wants to guess $X$ correctly always, regardless of whether $\Theta = 0$ or $\Theta = 1$. This means that she requires, in particular, that $P_{\text{guess}}(X|\Theta = 0) = 1$, Eve should prepare a state that will always produce a deterministic outcome when Alice measures in the standard basis. In earlier weeks, we have seen that for this to happen, Eve can for example send the state $|0\rangle\langle 0|_A$, where Alice, upon measuring in the standard basis, will always produce $X = 0$. However, if Eve has used the strategy of preparing $|0\rangle\langle 0|_A$, what happens when Alice now measured in the Hadamard basis instead? We can calculate the probability

$$P_{\text{guess}}(X|\Theta=1) = \max\left[\, p(X=0|\Theta=1), p(X=1|\Theta=1)\,\right] \tag{3.50}$$

$$= \max\left[\, \operatorname{tr}\left(|+\rangle\langle+||0\rangle\langle 0|\right), \operatorname{tr}\left(|-\rangle\langle-||0\rangle\langle 0|\right)\,\right] = \frac{1}{2}. \tag{3.51}$$

Therefore, if Eve uses this strategy of preparing $\rho_A = |0\rangle\langle 0|_A$ in order to guess Alice's outcome $X$, then whenever $\Theta = 1$, this corresponds only to a random guess! What's important in this protocol is that since Eve does not know beforehand what basis Alice will choose to measure in, she has to prepare a state that will maximize her guessing probability in *both* cases of Alice measuring in the standard basis, and also the Hadamard basis. We have seen from the above example that this guessing probability can never be equal to 1.

Note that in order for Eve to maximize the guessing probability $P_{\text{guess}}(X|\Theta)$ over $\rho_A$ (without loss of generality one can consider the outcome to be $X = 0$),

$$P_{\text{guess}}(X|\Theta) = \frac{1}{2}\cdot[\operatorname{tr}(\rho_A|0\rangle\langle 0| + \operatorname{tr}(\rho_A|+\rangle\langle+|))] \tag{3.52}$$

$$= \frac{1}{2}\cdot\operatorname{tr}\left[\rho_A(|0\rangle\langle 0| + |+\rangle\langle+|)\right]. \tag{3.53}$$

then she has to prepare $\rho_A$ in the pure state corresponding to the eigenvector of $|0\rangle\langle 0| + |+\rangle\langle+|$ with the largest eigenvalue. Check for yourselves that the largest eigenvalue of this matrix is $\lambda_{\max} = 1 + \frac{1}{\sqrt{2}}$. Therefore, we have that $P_{\text{guess}}(X|\Theta) = \frac{1}{2} + \frac{1}{2\sqrt{2}} < 1$.

### 3.4.1 Analysis: winning probability of the guessing game

Let us first try to calculate Eve's guessing probability for the protocol in Def. 3.4.1. We have seen in previous lectures that any state can be written in its Bloch representation as $\rho_A = \frac{1}{2}(\mathbb{I} + v_x X + v_y Y + v_z Z)$, where the vector $\vec{v} = (v_x, v_y, v_z)$ is a 3-dimensional real vector. Therefore, one may calculate the following inner products using the Bloch representation:

$$\operatorname{tr}(\rho_A|0\rangle\langle 0|) = \frac{1}{2}(1+v_z), \qquad \operatorname{tr}(\rho_A|1\rangle\langle 1|) = \frac{1}{2}(1-v_z), \tag{3.54}$$

$$\operatorname{tr}(\rho_A|+\rangle\langle+|) = \frac{1}{2}(1+v_x), \qquad \operatorname{tr}(\rho_A|-\rangle\langle-|) = \frac{1}{2}(1-v_x). \tag{3.55}$$

On the other hand,

$$p_{\text{guess}}(X|\Theta) = \frac{1}{2}\max\{\operatorname{tr}(\rho_A|0\rangle\langle 0|), \operatorname{tr}(\rho_A|1\rangle\langle 1|)\} + \frac{1}{2}\max\{\operatorname{tr}(\rho_A|+\rangle\langle+|), \operatorname{tr}(\rho_A|-\rangle\langle-|)\}, \tag{3.56}$$

where we want this value maximized over all possible states $\rho_A$, since Eve is allowed to pick any arbitrary state. Since the maximizations of both expression are symmetric around $v_z = 0, v_x = 0$ respectively, we can without loss of generality consider only the case where $v_z, v_x \geq 0$. The expression in Eq. (3.56) then reduces to

$$p_{\text{guess}}(X|\Theta)_{\rho_A} = \frac{1}{2}\operatorname{tr}\left[\rho_A\left(|0\rangle\langle 0| + |+\rangle\langle+|\right)\right] = \frac{1}{4}(2+v_z+v_x), \qquad v_z^2 + v_x^2 \leq 1. \tag{3.57}$$

To maximize this expression over all states $\rho_A$ implies maximizing Eq. (3.57) over the constraint $v_z^2 + v_x^2 \leq 1$, and the maximum happens only when $v_z^2 + v_x^2 = 1$ (this implies that $\rho_A$ is pure for Eve's optimal strategy). Using the parametrization $v_z = \sin t, v_x = \cos t$ then gives us that

$$\max_t\,(\sin t + \cos t), \qquad \text{achieved when } \sin t = \cos t = \frac{1}{\sqrt{2}}. \tag{3.58}$$

Therefore, the probability Eve wins this game is $P_{\text{guess}}(X|\Theta)_{\rho_A} = 1/2 + 1/(2\sqrt{2}) \approx 0.85$.

In a more general scenario, Eve may even have classical information about $\rho_A$. This means that she is able to create an arbitrary cq-state $\rho_{AC} = \sum_c p_c \rho_c^A \otimes |c\rangle\langle c|_C$ according to some distribution $\{p_c\}_c$, and sends $\rho_A = \sum_c p_c \rho_c^A$ to Alice while keeping the classical label $C$. Let us further convince ourselves that any further classical information Eve holds about $\rho_A$ does not help. Suppose that Eve can prepare any cq-state $\rho_{AC} = \sum_c p_c \rho_c^A \otimes |c\rangle\langle c|_C$, and sends $\rho_A$ to Alice. The guessing probability further conditioned on $C$ is given by

$$p_{\text{guess}}(X|\Theta C)_{\rho_{AC}} = \sum_c p_c p_{\text{guess}}(X|\Theta)_{\rho_c^A} \tag{3.59}$$

where we maximize over all possible $\{p_c, \rho_c^A\}_c$. But we have previously already shown the maximum possible value of $p_{\text{guess}}(X|\Theta)_{\rho_c^A}$, over all possible $\rho_c^A$! Therefore, Eq. (3.59) yields

$$p_{\text{guess}}(X|\Theta C)_{\rho_{AC}} = \frac{1}{2}\left(1 + \frac{1}{\sqrt{2}}\right) \approx 0.85. \tag{3.60}$$

This quantity $P_{\text{guess}}(X|\Theta C)$ now directly tells us about the min-entropy about this bit, since $H_{\min}(X|\Theta C) = -\log P_{\text{guess}}(X|\Theta C)$. That gives a value for min-entropy per bit, of $H_{\min}(X|\Theta C) = -\log P_{\text{guess}}(X|\Theta C) \approx 0.22$.

Next, let us give Eve a little more power. Suppose that not only can Eve prepare a state $\rho_A$ for Alice to measure, she might create a larger state $\rho_{AE}$, possibly entangled, and send only $\rho_A$ to Alice. Note that since we always allow Eve maximum information about everything, $\rho_{AE}$ is always pure: Eve always holds the purification as well. We will thus simply assume that Eve can *prepare* pure states $\rho_{AE}$ of which she sends qubit $A$ to Alice.

**Exercise 3.4.1** Show that if Eve can keep entanglement, that is the can prepare an arbitrary entangled state $\rho_{AE}$ then she can guess $X$ perfectly.
Hint: consider the case where Eve prepares the EPR pair. ■

When you complete the exercise you will discover that if Eve can be entangled with Alice's qubit, then she can guess perfectly.

Is there any hope for security (i.e. keeping $X$ secret from Eve) at all then? The answer to this is yes: remember that entanglement is monogamous! In other words, if we want limit Eve's knowledge about Alice's measurement outcomes, then we need to use two aspects of quantum mechanics:

- Uncertainty: If Eve has no (or little) entanglement with Alice, then she cannot predict the outcomes of two incompatible measurements (very well). In particular, this means it is difficult for here to guess Alice's measurement outcomes, i.e., $P_{\text{guess}}(X|E\Theta) < 1$, or equivalently, $H_{\min}(X|E\Theta) > 0$.
- Entanglement: We need a means to ensure there actually is little entanglement between Alice and Eve. For this we can use the fact that entanglement is *monogamous*, that is, if we find a large amount of entanglement between Alice and Bob, then we know that Eve has very little entanglement with either Alice or Bob, and therefore the min-entropy should be large!

## 3.5 Extended uncertainty relation principles: A tripartite guessing game

In this section, in order to make use of the monogamous property of entanglement, we consider a direct extension of the guessing game as before, only this time we are given no guarantee about the entanglement (or absence thereof) between Alice and Eve. Instead, we have a third party Bob, whom Alice trusts. In particular, to show security against Eve, Alice and Bob may join forces to make an estimate of Eve's min-entropy. To do so, they need to perform an entanglement test between Alice and Bob to ensure that by the monogamy of quantum entanglement, the entanglement between Alice and Eve is small. For this, let us consider the following tripartite guessing game.

**Definition 3.5.1 — Tripartite guessing game - Alice, Bob and Eve.** Suppose Alice plays against Bob and Eve in the following way:

1. Eve prepares a global state $\rho_{ABE}$, and sends qubits $A$ and $B$ to Alice and Bob respectively.
2. Alice chooses a random bit $\Theta \in \{0,1\}$.
3. If $\Theta = 0$, then Alice measures $\rho_A$ in the standard basis; if $\Theta = 1$, then she measures in the Hadamard basis.
4. Alice obtains a measurement outcome $X \in \{0,1\}$ and records it.
5. Alice announces $\Theta$ to both Bob and Eve.
6. Given $\Theta$, Bob measures $\rho_B$ and makes a guess $\tilde{X}$. Likewise, Eve measures $\rho_E$ and makes a guess $X_E$.
7. Bob and Eve win the game if $X_E = X = \tilde{X}$.

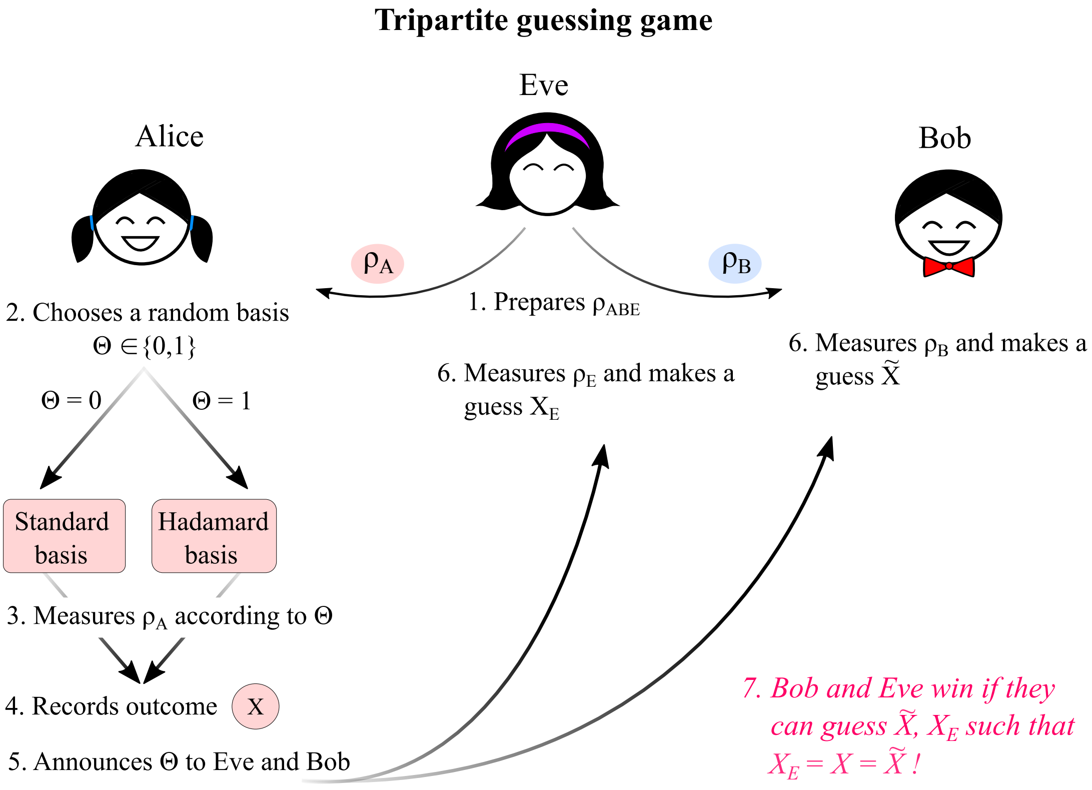
Tripartite guessing game
Eve
Alice
Bob
$\rho_A$
$\rho_B$
1. Prepares $\rho_{ABE}$
2. Chooses a random basis $\Theta \in \{0,1\}$
$\Theta = 0$
$\Theta = 1$
Standard basis
Hadamard basis
3. Measures $\rho_A$ according to $\Theta$
4. Records outcome
X
5. Announces $\Theta$ to Eve and Bob
6. Measures $\rho_E$ and makes a guess $X_E$
6. Measures $\rho_B$ and makes a guess $\tilde{X}$
7. Bob and Eve win if they can guess $\tilde{X}$, $X_E$ such that $X_E = X = \tilde{X}$ !

Figure 3.3: A tripartite guessing game where Eve gets to prepare the global state $\rho_{ABE}$. She send the qubits $A$ and $B$ to Alice and Bob respectively, where Alice measures randomly in either the standard or Hadamard basis. Bob and Eve both provide guesses $\tilde{X}, X_E$, and we say that they win the game if $X_E = X = \tilde{X}$.

Therefore, our goal will be to bound the probability that they all produce the same outcome, averaged over the choice of basis, that is, that Bob and Eve wins the guessing game.

$$p_{\text{Tripartite}} = p\left(X = \tilde{X} = X_E\right) = \sum_{\Theta\in\{0,1\}} p_\Theta p(X = \tilde{X} = X_E|\Theta) \tag{3.61}$$

$$= \frac{1}{2}\sum_{\theta\in\{0,1\}} \operatorname{tr}\left[\rho_{ABE}\left(\sum_{x\in\{0,1\}} |x\rangle\langle x|_\theta^A \otimes |x\rangle\langle x|_\theta^B \otimes M_{x|\theta}^E\right)\right] , \tag{3.62}$$

where we used superscripts $A$, $B$ and $E$ to denote the systems on which we perform the measurements, and $|x\rangle_\Theta$ to denote basis element $x$ in the basis $\Theta$. That is, $|0\rangle_0 = |0\rangle$, $|1\rangle_1 = |1\rangle$, and $|0\rangle_1 = |+\rangle$, $|1\rangle_1 = |-\rangle$. The probability above is the probability that they all give the same outcome $x$ when measuring the state $\rho_{ABE}$. Of course, we don't know anything about the state $\rho_{ABE}$ or the measurement $\{M_{x|\Theta}^E\}_x$ with outcomes $x$ that Eve will perform on $E$ depending on the basis $\Theta$. We only know that this must be a quantum state, and Eve can only make measurements that are allowed by the laws of quantum mechanics. Since it is known that all POVMs can be realized as projective measurements using a potentially larger ancilla, and our all powerful Eve can hold the entire rest of the universe except Alice and Bob's labs, we can without loss of generality assume that Eve's measurements are projective. Given her access to a smaller space only makes things more difficult for Eve and in a security analysis we are always allowed to make the adversary more (but not less!) powerful.

### 3.5.1 Analysis: winning probability of the tripartite guessing game

How could we hope to analyze this situation? Previously when we considered a classical Eve, the solution was given by a simple eigenvalue problem, and if we would fix Eve's measurements then again we obtain an eigenvalue problem

$$\max_{\rho_{ABE}} \operatorname{tr}\left[\rho_{ABE}\left(\frac{1}{2}\sum_\Theta \Pi_\Theta\right)\right] , \tag{3.63}$$

where

$$\Pi_\Theta = \sum_{x\in\{0,1\}} |x\rangle\langle x|_\Theta^A \otimes |x\rangle\langle x|_\Theta^B \otimes M_{x|\Theta}^E . \tag{3.64}$$

Now we are in some small amount of trouble given that we don't know $M_{x|\Theta}^E$ and malicious Eve will of course use the best possible measurements.

#### Two tools from linear algebra

To get around this dificulty, we will use two little linear algebra tricks which are proven in [Tom+13]. To write them down, let us first introduce a shorthand for the maximization problem above. In general, the *operator norm* of some operator $O$, can be written as

$$\|O\|_\infty = \max_\rho \operatorname{tr}[\rho O] , \tag{3.65}$$

where the maximization is taken over all $\rho$ such that $\operatorname{tr}[\rho] \leq 1$. When, $O$ is Hermitian, then we just maximize over all quantum states $\rho$, that is, $\rho$ satisfying $\rho \geq 0$ and $\operatorname{tr}[\rho] = 1$. Note that this means we can reduce the maximization problem above to studying

$$\left\|\frac{1}{2}\sum_{\theta\in\{0,1\}} \Pi_\theta\right\|_\infty , \tag{3.66}$$

for of course still partially unknown $\Pi_\theta$. When talking about operators, people often omit the subscript $\infty$ and simply write $\|O\| = \|O\|_\infty$ as is also done in [Tom+13], and we will use this simpler notation from now on. Nevertheless, while cumbersome, one can establish the following two facts:

1. For any two projectors $\Pi_0$ and $\Pi_1$ [1], we have

$$||\Pi_0 + \Pi_1|| \leq \max\{||\Pi_0||, ||\Pi_1||\} + ||\Pi_0\Pi_1||. \tag{3.67}$$

([Tom+13, Lemma 2])

2. If $\Pi_0 \leq P$ and $\Pi_1 \leq Q$ [2], then $||\Pi_0\Pi_1|| \leq ||PQP||$.

([Tom+13, Lemma 1])

Let us now use these two tricks to bound Eve's probability of winning. Using trick 1, we have that

$$\max_{M^E} \left\| \frac{1}{2} \sum_{\theta\in\{0,1\}} \Pi_\theta \right\|_\infty = \max_{M^E} \frac{1}{2} \left\| \sum_{\theta\in\{0,1\}} \Pi_\theta \right\|_\infty \tag{3.68}$$

$$\leq \frac{1}{2}\left(1 + \max_{M^E} ||\Pi_0\Pi_1||\right) , \tag{3.69}$$

where we have used that $||\Pi_0||, ||\Pi_1|| \leq 1$ for any measurements $M^E$ that Eve could make in quantum mechanics (convince yourself that this is true!). It remains to analyze $||\Pi_0\Pi_1||$ for which we will use trick number two, for some smart choice of $P$ and $Q$. Note that since all measurement operators $M^E_{x|\theta} \leq \mathbb{I}$ and also $|x\rangle\langle x|_\theta \leq \mathbb{I}$, we have that

$$\Pi_0 \leq \sum_{x\in\{0,1\}} |x\rangle\langle x|_0^A \otimes |x\rangle\langle x|_0^B \otimes \mathbb{I}^E =: P \tag{3.70}$$

$$\Pi_1 \leq \sum_{x\in\{0,1\}} |x\rangle\langle x|_1^A \otimes \mathbb{I}^B \otimes M^E_{x|1} =: Q \tag{3.71}$$

Using the fact that $\langle x|y\rangle = 0$ if $x \neq y$ in the same basis, and that $\sum_y M^E_{y|1} = \mathbb{I}$ for any quantum measurement Eve may make, we thus have

$$PQP = \sum_{x,y,z} |x\rangle\langle x|_0^A|y\rangle\langle y|_1^A|z\rangle\langle z|_0^A \otimes |x\rangle\langle x|_0^B|z\rangle\langle z|_0^B \otimes M^E_{y|1} \tag{3.72}$$

$$= \sum_{x,y} \frac{1}{2} |x\rangle\langle x|_0^A \otimes |x\rangle\langle x|_0^B \otimes M^E_{y|1} \tag{3.73}$$

$$= \frac{1}{2}\sum_x |x\rangle\langle x|_0^A \otimes |x\rangle\langle x|_0^B \otimes \sum_y M^E_{y|1} \tag{3.74}$$

$$= \frac{1}{2}\sum_x |x\rangle\langle x|_0^A \otimes |x\rangle\langle x|_0^B \otimes \mathbb{I}^E \ . \tag{3.75}$$

This gives $||PQP|| \leq 1/2$. Using trick number two, and plugging into Eq. (3.69) we thus have that

$$p_{\text{Tripartite}} \leq \frac{1}{2}\left(1 + \frac{1}{\sqrt{2}}\right) = \frac{1}{2} + \frac{1}{2\sqrt{2}} , \tag{3.76}$$

which is again our familiar number from the much simpler guessing game, where Eve was all classical! Moreover, it can be shown using messy but not not more advanced mathematical tools that also when we consider collective attacks

$$p^{\text{n rounds}}_{\text{Tripartite}} \leq \left(\frac{1}{2} + \frac{1}{2\sqrt{2}}\right)^n , \tag{3.77}$$

[1] Recall that a projector $\Pi$ is an operator such that $\Pi^2 = \Pi$.

[2] Recall that $A \leq B$ means that $B - A \geq 0$.

and she can achieve this bound by playing the optimal one round strategy!

We thus know that if the error rate is low, and Bob can reproduce a significant fraction $X = \tilde{X}$, then it is difficult for Eve to guess $X_E = X$ and hence her min-entropy must be large.

## Acknowledgements

This work is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International Licence. The lecture notes are written by Stephanie Wehner, Nelly Ng, and Thomas Vidick. We thank David Elkouss, Jonas Helsen, Jérémy Ribeiro and Kenneth Goodenough for proofreading.

## Important identities for calculations

### Trace distance

$$D(\rho_{\text{real}}, \rho_{\text{ideal}}) := \max_{0 \leq M \leq \mathbb{I}} \operatorname{tr}\left[M\left(\rho_{\text{real}} - \rho_{\text{ideal}}\right)\right] \tag{3.78}$$

$$= \frac{1}{2} \operatorname{tr}\left[\sqrt{A^\dagger A}\right], \qquad A = \rho_{\text{real}} - \rho_{\text{ideal}}. \tag{3.79}$$

Properties:

1. $D(\rho, \rho') \geq 0$ with equality iff $\rho = \rho'$.
2. $D(\rho, \rho') = D(\rho', \rho)$.
3. $D(\rho, \rho') + D(\rho', \rho'') \geq D(\rho, \rho'')$.
4. $D(\sum_i p_i \rho_i, \sigma) \leq \sum_i p_i D(\rho_i, \sigma)$.

### Fidelity

$$F(\rho, \rho') := \operatorname{tr}\left[\sqrt{\sqrt{\rho}\rho'\sqrt{\rho}}\right]. \tag{3.80}$$

If $\rho = |\psi\rangle\langle\psi|$ and $\rho' = |\psi'\rangle\langle\psi'|$, then $F(|\psi\rangle\langle\psi|, |\psi'\rangle\langle\psi'|) = \sqrt{\langle\Psi_1|\rho_2|\Psi_1\rangle}$.
Relation to trace distance: $1 - F \leq D \leq \sqrt{1 - F^2}$.

### Min-entropy

Unconditional : $\mathrm{H}_{\min}(X) = \mathrm{H}_{\min}(\rho_X) = -\log \max_x p_x$ .
Conditional : For a cq-state $\rho_{XE}$, $\mathrm{H}_{\min}(X|E) := -\log P_{\text{guess}}(X|E)$, where

$$P_{\text{guess}}(X|E) := \max_{\{M_x\}_x} \sum_x p_x \operatorname{tr}\left[M_x \rho_x^E\right], \{M_x \geq 0 \,|\, \sum_x M_x = \mathbb{I}\}.$$

Properties:

1. $0 \leq \mathrm{H}_{\min}(X|E) \leq \mathrm{H}_{\min}(X) \leq \log|X|$, but only for cq states! For quantum register $X$, $\mathrm{H}_{\min}(X|E)$ can be negative.
2. $\mathrm{H}_{\min}(X|E) \geq \mathrm{H}_{\min}(X) - \log|E|$.

### A secret key

A key $K$ is secret from Eve iff it is *uniform and uncorrelated* from Eve, i.e. the joint state $\rho_{KE}$ is of the form

$$\rho_{KE} = \frac{\mathbb{I}_K}{d_K} \otimes \rho_E. \tag{3.81}$$

# Bibliography

[FV99] Christopher A Fuchs and Jeroen Van De Graaf. “Cryptographic distinguishability measures for quantum-mechanical states”. In: *IEEE Transactions on Information Theory* 45.4 (1999), pages 1216–1227 (cited on page 5).

[Hel76] Carl W. Helstrom. *Quantum detection and estimation theory / Carl W. Helstrom*. English. Academic Press New York, 1976, ix, 309 p. : ISBN: 0123400503 (cited on page 3).

[KRS09] Robert Konig, Renato Renner, and Christian Schaffner. “The operational meaning of min-and max-entropy”. In: *IEEE Transactions on Information theory* 55.9 (2009), pages 4337–4347 (cited on page 9).

[Ren08] Renato Renner. “Security of quantum key distribution”. In: *International Journal of Quantum Information* 6.01 (2008), pages 1–127 (cited on page 7).

[Tom+13] M. Tomamichel et al. “A Monogamy-of-Entanglement Game With Applications to Device-Independent Quantum Cryptography”. In: *New Journal of Physics* 15 (2013). EUROCRYPT 2013, arXiv:1210.4359, page 103002 (cited on pages 16, 17).