Quantum Aspects of Cryptography

Assignment 1—Quantum Review
(For lectures 1, 2 and 3)
Assigned: Thursday, Jan 23, 2025
Due (2 weeks): Thursday, Feb 6, 2025

Instructions.

1. You are encouraged to write to me to setup a meeting should something not be clear.
2. Medium
   (a) If you prefer to type your answers:
      i. Please record your screen showing your work (ensure there is a video feed that clearly shows your face).
      ii. Upload this recording Google Drive/YouTube etc. with appropriate privacy settings, and obtain a shareable link.
      iii. Include this link in the final PDF.

   (b) If you handwrite your answers, the aforementioned steps are not needed. However, you must submit a scanned PDF of your answers before the deadline. Please use a dedicated scanning app or a scanner if you have access to one—but do not submit photos as they are hard to print.

   In both cases:

   (a) Please include the assignment number, together with your name, email and enrolment number in the PDF.
   (b) If your name is *Alice* and you're submitting answers to *Assignment 1*, use `Alice1.pdf` as your filename when submitting.
   (c) Submit your assignment using this OneDrive link for Assignment 1.
3. You can cooperate among yourselves but understand and write the answers yourself. If two (or more) submissions have *identical* answers, both submissions will lose all points for that answer.
4. At most one late submission (by one week), at most once a month (once in January, once in February and so on) is allowed without penality—granted an extension was sought before the deadline. For instance if an extension is sought for an assignment that was assigned on Jan 23, then this is counted towards a late submission in January.
5. Grading: We will hold a *long tutorial session*, once before the mid-semester, and once before the final exam. Each of these long tutorials will consist of three parts.
   (a) Final clarification. To answer any questions you may have regarding the assignments or the upcoming exam.
   (b) Peer review part. You will receive a link to the answers submitted by one of your peers. You will also get a printed score card where you have to award points from 0 to 5 to each item in each exercise (E.g. If Exercise 1 has three sub-exercises, each sub-exercise gets 5 points.).
   Guideline for grading:
      i. A score of 5 should mean that the question was answered *correctly* and *explained well.*
      ii. A score of 3 could mean that a partial answer was given or that even though the answer looks like it could be correct, it is hard to gauge with confidence due to lack of details/poor presentation.
      iii. A score of 0 should mean that no relevant progress was made at answering the question.
      iv. Flag any question that looks like it was copied without understanding.

   (c) Viva voce: We will have a viva voce exam where I'll ask you to present a random (not necessarily uniformly random) subset of your assignment answers. The goal is to make sure you actually understood what you wrote and give you a chance to increase your score if you can answer a question you got wrong in your submission.

Elementary exercises.

Exercise 1. Prove the following to ensure the notation is clear:

1. For a matrix $H \in \mathbb{C}^{d\times d}$ and a ket $|\psi\rangle \in \mathbb{C}^d$,
$$(H|\psi\rangle)^\dagger = \langle\psi| H^\dagger.$$

2. The vector
$$|\psi\rangle = \frac{|1\rangle + |2\rangle + \dots |d\rangle}{\sqrt{d}}$$
is normalised. The matrix $\Pi = \sum_{i,j=1}^d \frac{|i\rangle\langle j|}{d}$ can be expressed in a very simple form in terms of $|\psi\rangle$. Finally, Π satisfies $\Pi^2 = \Pi$ and has rank 1.

3. For any two orthonormal basis $\{|u_1\rangle \dots |u_d\rangle\}$ and $\{|v_1\rangle \dots |v_d\rangle\}$, there is a (unique) unitary matrix U such that $U|u_i\rangle = |v_i\rangle$ for all $i \in \{1 \dots d\}$.

Exercise 2. Prove the following.

1. Every Hermitian matrix H has real eigenvalues.

2. If λ is an eigenvalue of a unitary matrix U, then $|\lambda| = 1$.

3. If λ is an eigenvalue of a projector Π (i.e. a matrix satisfying $\Pi^2 = \Pi$), then λ is either 1 or 0.

Exercise 3. Verify that the expected result of measuring O when the system is in the state $|\psi\rangle$ is $\langle\psi| O |\psi\rangle$ which is sometimes briefly written as $\langle O\rangle$.

Exercise 4. Let σ_x, σ_y and σ_z be Pauli matrices (use the convention from class). Then, show that
$$\begin{aligned} [\sigma_z, \sigma_x] &= 2i\sigma_y \\ [\sigma_y, \sigma_z] &= 2i\sigma_x \\ [\sigma_x, \sigma_y] &= 2i\sigma_z \end{aligned}$$

Also, verify that for all $\tau \in \{\sigma_x, \sigma_y, \sigma_z\}$,

1. $\tau^2 = \mathbb{I}$ and so $[\tau, \tau] = 0$,

2. $\det(\tau) = -1$ and $\mathsf{tr}(\tau) = 0$.

Exercise 5. Let O_1, O_2 be as above and let $|\psi\rangle \in \mathbb{C}^d$ denote any quantum state. Consider the following experiments:

1. Measure O_1 first, to obtain o_1 and then measure O_2 to obtain o_2

2. Measure O_2 first, to obtain o_2 and then measure O_1 to obtain o_1

Prove that the probability one obtains $o_1 = a$ and $o_2 = b$ is the same in both cases, i.e.
$$\Pr[(o_1, o_2) = (a, b) : \text{Experiment 1}] = \Pr[(o_1, o_2) = (a, b) : \text{Experiment 2}]$$
for all $a \in \text{spectrum}(O_1)$ and all $b \in \text{spectrum}(O_2)$.

Exercise 6. Understand what the Mach-Zhander interferometer is. Can one view it as a simplification of the Double-Slit experiment (as discussed in class)? Explain the observations made using a Mach-Zhander interferometer starting from the postulates of quantum mechanics.

Exercise 7. If $\{|x_i\rangle\}_{i\in I}$ and $\{|y_j\rangle\}_{j\in J}$ are orthonormal bases for vector spaces $\mathcal{X}$ and $\mathcal{Y}$ respectively, then $\{|x_i\rangle \otimes |y_j\rangle\}_{i\in I, j\in J}$ spans the vector space $\mathcal{X} \otimes \mathcal{Y}$.

Exercise 8. Explicitly write down the tensor products assuming systems A and B are both two-dimensional:

1. $\mathbb{I}_A \otimes \mathbb{I}_B$

2. $\mathbb{I}_A \otimes (\sigma_x)_B$

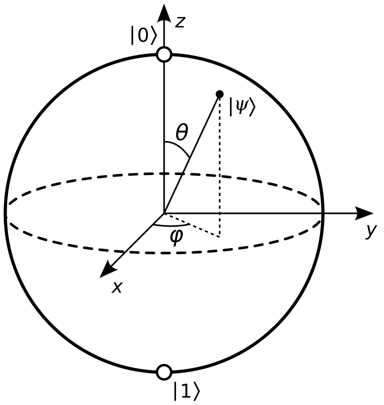

Figure 1: Bloch Sphere (taken from Wikipedia)

3. $(\sigma_x)_A \otimes (\sigma_x)_B$
4. $(\sigma_x)_A \otimes (\sigma_z)_B$

Exercise 9. Prove that for any state $|\psi\rangle \in \mathbb{C}^d$ and any matrix $O \in \mathbb{C}^{d\times d}$, $\langle\psi| O |\psi\rangle = \mathsf{tr}(O|\psi\rangle\langle\psi|)$.

Exercise 10. Let $\rho := \frac{3}{4}|0\rangle\langle 0| + \frac{1}{4}|1\rangle\langle 1|$ and $\sigma := \frac{1}{2}|u\rangle\langle u| + \frac{1}{2}|v\rangle\langle v|$ where $|u\rangle := \sqrt{3/4}\,|0\rangle + \sqrt{1/4}\,|1\rangle$ and $|v\rangle := \sqrt{3/4}\,|0\rangle - \sqrt{1/4}\,|1\rangle$. If $\rho = \sigma$, show this explicitly. If $\rho \neq \sigma$, prove it.

Exercise 11. Prove that ρ_{S} is indeed a density matrix, if ρ_{SE} is a density matrix where SE are two registers.

Exercise 12. Let AB be registers with $\mathcal{A}$ and $\mathcal{B}$ both $\mathbb{C}^2$. Write down the density matrix ρ_{AB} and the reduced density matrix ρ_{B} corresponding to the following pure states.

1. $|\psi\rangle_{\mathsf{A}} \otimes |\phi\rangle_{\mathsf{B}}$
2. $\sqrt{p_0}\,|0\rangle_{\mathsf{A}} \otimes |\psi_0\rangle_{\mathsf{B}} + \sqrt{p_1}\,|1\rangle_{\mathsf{A}} \otimes |\psi_1\rangle_{\mathsf{B}}$ where $p_0 \leq 1$ and $p_1 = 1 - p_0$.
3. $(|00\rangle + |11\rangle)_{\mathsf{AB}}/\sqrt{2}$.

Exercise 13 (Purification)**.** Let $\rho_{\mathsf{A}} = \sum_{i\in I} \lambda_i |u_i\rangle\langle u_i|_{\mathsf{A}}$ be the spectral decomposition of a density matrix $\rho_{\mathsf{A}} \in \mathcal{A}$. Then, verify that $|\psi\rangle_{\mathsf{AB}} = \sum_{i\in I}\sqrt{\lambda_i}\,|u_i\rangle_{\mathsf{A}}|i\rangle_{\mathsf{B}}$ satisfies $\mathsf{tr}_{\mathsf{B}}(|\psi\rangle\langle\psi|_{\mathsf{AB}}) = \rho_{\mathsf{A}}$. Is there any other state satisfying this property? Give an example.

Exercise 14 (Simple facts about the Bloch sphere)**.** Show the following simple facts about the Bloch sphere.

1. Warmup:
   (a) Show that a qubit in an arbitrary pure state $|\psi\rangle$ can be written as $|\psi\rangle = \cos(\theta/2)\,|0\rangle + e^{i\phi}\sin(\theta/2)\,|1\rangle$. How did you decide the range of θ and ϕ? Recall this is what we called the *Bloch Sphere* representation.
   (b) Find the normalised eigenvectors of $\sigma_x, \sigma_y, \sigma_z$.
   (c) Represent the state $\frac{1}{2}\left(|0\rangle + e^{i\pi/4}\sqrt{3}\,|1\rangle\right)$ on the Bloch sphere.
   (d) Show that opposite points on the Bloch sphere correspond to orthogonal states.
2. Consider the observable $\hat{n}\cdot\vec{\sigma}$ where $\hat{n} = (n_x, n_y, n_z)$ is a normalised vector and $\vec{\sigma} := (\sigma_x, \sigma_y, \sigma_z)$ is an ordered pair of Pauli matrices.
   (a) Show that $\hat{n}\cdot\vec{\sigma}$ has eigenvalues ± 1 and that the projectors on the corresponding eigenspaces are $P_{\pm} := (\mathbb{I} \pm \hat{n}\cdot\vec{\sigma})/2$.
   (b) Compute the probability to get the outcome $+1$ for a measurement of $\hat{n}\cdot\vec{\sigma}$ on the state $|0\rangle$.
   (c) Where does the post measurement state lie on the Bloch sphere?

Exercise 15 (No cloning)**.** Show that there cannot exist a unitary U acting on $\mathcal{H}\otimes\mathcal{H}$ that maps $|\psi\rangle\otimes|0\rangle$ to $|\psi\rangle\otimes|\psi\rangle$.

Less elementary exercises. Try to think about the problem yourself before looking up solutions, if you must.

Exercise 16 (Uniqueness of partial trace)**.** Consider two registers AB and suppose M is a (projective) measurement on system A and $\tilde{M}$ denotes the same measurement applied to the joint system AB.

1. Prove that $\tilde{M} = M \otimes \mathbb{I}_B$. Argue by considering projectors and taking the system to be in the state $|m\rangle_A \otimes |\psi\rangle_B$ where $|m\rangle$ is an eigenstate of M.
2. Show that for any $\rho_{AB} \in \mathcal{A} \otimes \mathcal{B}$, it holds that
$$\mathsf{tr}(M\rho_A) = \mathsf{tr}(\tilde{M}\rho_{AB}) = \mathsf{tr}((M \otimes \mathbb{I}_B)\rho_{AB}) \tag{1}$$
where $\rho_A := \mathsf{tr}_B \rho_{AB}$.
3. Let f be any map that takes density matrices in $\mathcal{A} \otimes \mathcal{B}$ to density matrices in $\mathcal{A}$. Prove that if $\mathsf{tr}(Mf(\rho_{AB})) = \mathsf{tr}(\tilde{M}\rho_{AB})$ for all ρ_{AB}, then f uniquely specifies the partial trace, i.e. $\mathsf{tr}_B(\cdot)$.
Hint: use an orthonormal basis of operators M_i for the space of Hermitian operators, with respect to the Hilbert-Schmidt inner product, $(X, Y) := \mathsf{tr}(XY)$ and Equation (1).

Bit commitment. Here is semi-formal description of (a variant of) *bit-commitment*, in the classical setting. A bit-commitment protocol involves two parties Alice and Bob and it has two phases: the commit phase and the reveal phase.

In the commit phase, Alice chooses a bit $a \in \{0, 1\}$ and 'commits' to it by producing a string s_a and sending it to Bob. (Think of s_a as locking the answer in a safe and giving the safe—but not the combination—to Bob.)

In the reveal phase, Alice reveals the 'opening' r to the commitment s_a. Using (r, s_a) Bob can recover a (or output $\perp$ if the pair (r, s_a) is invalid). (Think of r as the combination to the safe.)

A bit commitment protocol must satisfy two properties:

1. Binding.
Suppose both Alice and Bob follow the protocol honestly but Alice becomes malicious in the reveal phase.
Alice should not be able to produce an opening r that opens to both $a = 0$ and $a = 1$.
2. Hiding.
Suppose Alice follows the protocol honestly, but Bob is malicious.
Bob should not be able to learn anything about the bit a from the commitment string s_a before the reveal phase starts.

Exercise 17. Suppose Alice and Bob have no bounds on their computational resources. Consider the following two cases:

1. Show that bit-commitment is impossible if both Alice and Bob are classical, i.e. both binding and hiding cannot simultaneously hold. You may argue as follows.
   (a) Suppose the scheme satisfies the binding property. Then for a given s_a, can there be any r that reveals $\neg a$ (instead of a)?
   What can you say about the relation between the set of possible strings sent by Alice when $a = 0$ and $a = 1$, i.e. $\{s_0\}$ and $\{s_1\}$ resp.?
   (b) Using your answer above, can you show that Bob can always learn b from s_b.
2. Show the same when they are both quantum by proceeding as follows.
   (a) Suppose Alice prepares a state $|\phi_b\rangle$ on registers AB and sends register B to Bob. Denote by ρ_b the reduced state on register B.
   (b) What does the hiding property say about the relation between ρ_0 and ρ_1?
   (c) What does Uhlman's theorem say about transforming purifications of a density matrix ρ? How are they related?
   (d) What does this observation say about the binding property of the commitment scheme?

Exercise 18 ('Data processing')**.** Let $\mathcal{E}$ be any completely positive trace preserving map from $\mathcal{H}$ to $\mathcal{H}'$ and suppose ρ and σ are density operators in $\mathsf{Pos}(\mathcal{H})$. Then, prove that[1]
$$\mathsf{TD}(\mathcal{E}(\rho), \mathcal{E}(\sigma)) \leq \mathsf{TD}(\rho, \sigma) \tag{2}$$
where recall that $\mathsf{TD}(X, Y) := \frac{1}{2} \|X - Y\|_1$. What connection do you see between Equation (2) and Figure 2?

[1] This is Theorem 9.2 in Neilsen and Chuang, 10th edition.

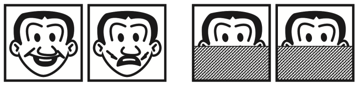

Figure 2: Data processing inequality (taken from Neilsen and Chuang).

Exercise 19 (Fidelity)**.** Recall that the fidelity between ρ and σ is defined as $F(\rho, \sigma) = \mathsf{tr}\left(\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}}\right)$.

1. Prove that $F(\rho, \sigma) = F(\sigma, \rho)$ and that $F(|\psi\rangle, \rho) = \sqrt{\langle\psi| \rho |\psi\rangle}$.
2. Understand and write down the proof of *Uhlmann's theorem (about fidelities)*, i.e. $F(\rho, \sigma) = \max_{|\psi\rangle, |\phi\rangle} |\langle\psi|\phi\rangle|$ where $|\psi\rangle, |\phi\rangle$ are purifications of ρ, σ respectively, e.g. from Neilsen Chuang, Theorem 9.4, 10th edition (prove the intermediate lemmas and exercises if you use them in the proof).
3. Show that for pure states, $\mathsf{TD}(|\psi\rangle, |\phi\rangle) = \sqrt{1 - F(|\psi\rangle, |\phi\rangle)^2}$.
4. Using Equation (2) with $\mathcal{E}$ as the partial trace and the points above[2] show that $\mathsf{TD}(\rho, \sigma) \leq \sqrt{1 - F(\rho, \sigma)^2}$.

[2] Specifically that there exist purifications $|\psi\rangle, |\phi\rangle$ such that $F(\rho, \sigma) = |\langle\psi|\phi\rangle| = F(|\psi\rangle, |\phi\rangle)$.