6.S895: Quantum Cryptography

Lecture 1: Introduction to Quantum Cryptography

Lecturer: Anand Natarajan **Scribe:** Vinod Vaikuntanathan

1 Why Quantum Cryptography?

Why study quantum cryptography? And why now—when, despite enormous progress on the hardware side, we are still far from having a working universal quantum computer?

We believe that the case for cryptographers to study quantum cryptography is clear: we live in a quantum world, and cryptography in this world is fundamentally different from cryptography in a purely classical world. Moreover, we think that even people whose primary interest is in quantum information processing should be interested in quantum cryptography. There are several reasons for this.

- **Quantum information enables classically impossible cryptographic capabilities.** Quantum information behaves in a qualitatively different way from classical information. Already at the information theoretic level, this gives quantum systems nontrivial capabilities that are provably impossible in the classical world. Famous examples of *information-theoretic quantum cryptography* are quantum money and quantum key distribution, which exploit two uniquely quantum features: the *uncertainty principle* and the *no-cloning theorem*. Quantum key distribution is possible in the classical world,[1] albeit under unproven computational assumptions. Quantum money is simply not achievable in a classical world.

- **Quantum computation breaks many classical cryptosystems and, perhaps more subtly, invalidates certain proofs of security of cryptographic protocols.** Most modern cryptography is founded on computational complexity, and relies on the computational hardness of certain problems. We know that some problems that seem classically intractable can actually be solved efficiently with a quantum computer; most famously, Shor showed that a quantum computer can efficiently factor large numbers and solve the discrete logarithm problem, and thus break cryptosystems like RSA, El Gamal (both the finite field version and the elliptic curve version).

  In fact, just recovering the capabilities of classical cryptography in a quantum world is a subtle and nontrivial task—it turns out to be *not enough* to simply replace factoring with a different problem like Learning With Errors which is presumed to be hard to solve with quantum algorithms! This subfield of cryptography, which relies on tools and techniques from quantum computation, is often called *post-quantum cryptography*.

- **Classical-Quantum Interactions.** The usual questions from cryptography can be asked here, e.g. the questions of delegated computation and blind computation. But there are new questions as well, e.g. tests of quantumness that give a way for a classical computer to test whether a device is "really quantum".

- **Quantum Complexity Theory 2.0.** In a quantum world, it becomes meaningful to discuss computational problems with quantum inputs or outputs. For example: How hard is it to prepare a quantum state? How hard is to come up with a unitary map that maps certain quantum states to

[1] ... in a well-defined model with authenticated classical channels, in a sense that will be clear in a few lectures.

others? How hard is to learn a classical description from many copies of a quantum state? More recently, we have come to realize that these problems have a rich complexity theory of their own, and are a source of interesting new hardness assumptions for cryptography.

- **Connections to Fundamental Physics.** What does cryptography have to do with black holes? There are new, albeit speculative, connections between the two fields. We may get to this at the end of the class, or this might be a good project topic.

The Five Worlds of Quantum. There are several possibilities in between a fully classical and fully quantum world, and many interesting things are possible in the intermediate worlds.

1. **NoQuantum**. We are almost definitely not in this world.
2. **BB84**. A world where single qubit states can be prepared and transmitted over long distances. We are already almost here: for example, quantum key distribution protocols that work over long distances have been implemented.
3. **NISQworld** (noisy intermediate scale quantum computers). We are close to here, but don't know what we can do yet.
4. **Quantum Feudalism**: Only very specialized labs (e.g. Google, Microsoft, IBM) possess large-scale qauntum computers. Users can interact with them classically or via single-qubit communication.
5. **Quantumania (or, Quantomnia?)**: A world where everyone has quantum computers, our iPhones are quantum etc.

2 Quantum Basics

We start with the basics of quantum information and computation. Our goal here is not to be exhaustive, rather to give the reader enough background to understand the rest of the course. We will also introduce relevant mathematical tools along the way.

2.1 Linear Algebra

We refer the reader to [Wat18] for an extensive discussion of the relevant linear algebraic definitions and facts, and only recall the most important ones below. Let $\mathcal{X}$ be a finite-dimensional Hilbert space, typically a subspace of $\mathbb{C}^d$.

- The ket notation $|\psi\rangle$ will refer to a column vector in $\mathbb{C}^d$.
- The bra notation $\langle\psi|$ is the conjugate transpose of $|\psi\rangle$.
- $\overline{\psi}$ denotes the (component-wise) complex conjugate, and $\psi^\dagger$ is the complex conjugate transpose of a column vector ψ. (Some authors use ψ^* to refer to the complex conjugate or the conjugate transpose; we prefer to avoid the * notation.)
- Thus, $\langle\psi|\psi\rangle$ is the squared norm of $|\psi\rangle$, and $|\psi\rangle\langle\psi|$ is the outer product of $|\psi\rangle$ with itself, which we will often view as a rank-1 matrix in $\mathbb{C}^{d\times d}$. For example, a matrix M in this notation is $M = \sum_{i,j\in[d]} M_{i,j}\,|i\rangle\langle j|$.

For Hilbert spaces $\mathcal{X}$ and $\mathcal{X}'$, we define the following classes of linear operators.

- $\mathcal{L}(\mathcal{X}, \mathcal{X}')$ is the set of all linear operators from $\mathcal{X}$ to $\mathcal{X}'$, and $\mathcal{L}(\mathcal{X})$ the set of all linear operators from $\mathcal{X}$ to itself.
- $\mathcal{H}(\mathcal{X}) \subseteq \mathcal{L}(\mathcal{X})$ is the set of all Hermitian operators from $\mathcal{X}$ to itself, where $X \in \mathcal{L}(\mathcal{X})$ is Hermitian if $X = X^\dagger$. Hermitian matrices have real eigenvalues and can be diagonalized. That is, $X = UDU^\dagger$ where D is a diagonal matrix with real entries, and U is a unitary matrix.
- $\mathcal{P}(\mathcal{X}) \subseteq \mathcal{H}(\mathcal{X})$ is the set of all positive semi-definite operators (also called positive operators) from $\mathcal{X}$ to itself. An operator $X \in \mathcal{L}(\mathcal{X})$ is positive semi-definite if $X = Y^\dagger Y$ for some $Y \in \mathcal{L}(\mathcal{X})$. Equivalently:
  - for all $v \in \mathcal{X}$, $v^\dagger X v \geq 0$; or
  - all eigenvalues of X are non-negative.
- $\mathcal{S}(\mathcal{X}) \subseteq \mathcal{P}(\mathcal{X})$ is the set of all density matrices, i.e. positive operators with unit trace. The eigenvalues of such a matrix are all positive, and their sum, therefore the eigenvalues can be interpreted as probabilities.
- $\mathsf{Proj}(\mathcal{X}) \subseteq \mathcal{P}(\mathcal{X})$ is the set of all projection operators, i.e. the set of all $\Pi \in \mathcal{P}(\mathcal{X})$ where $\Pi^2 = \Pi$.
- $\mathcal{U}(\mathcal{X}) \subseteq L(\mathcal{X})$ is the set of all unitary operators, i.e. the set of all $U \in L(\mathcal{X})$ where $UU^\dagger = U^\dagger U = \mathbb{1}_{\mathcal{X}}$.

2.2 Quantum States

Pure States. A pure state is a unit vector in $|\psi\rangle \in \mathcal{X}$, a d-dimensional Hilbert space where d is the size of the state space. That is, $\langle\psi|\psi\rangle = 1$. When necessary, we will use subscripts to denote which registers contains a state, e.g. by indicating $|\psi\rangle_A$ to mean that the state $|\psi\rangle$ lives in register A.

We will ask questions of the following form:

- Given $|\psi\rangle_{AB}$ what is the state of the A register?
- How do we model classical randomness over quantum states, e.g. to say that the state of a quantum state is $|\psi_i\rangle$ with probability p_i.

Both questions have the same answer, the *density matrix*, an important notion in quantum information. Let's start with the notion of an ensemble of pure states.

Ensemble of Pure States. An ensemble of pure states, also called a *mixed state*, is a collection $\{p_i, |\psi_i\rangle\}_{i=1}^m$ where p_i are non-negative real numbers with $\sum_{i=1}^m p_i = 1$ and each $|\psi_i\rangle$ is a pure state. (The $|\psi_i\rangle$ are not necessarily orthogonal.)

Density Matrices. An ensemble of pure states is concisely modeled by a density matrix

$$\rho = \sum_{i=1}^{m} p_i |\psi_i\rangle \langle\psi_i| \in \mathcal{S}(\mathcal{X}) \tag{1}$$

which is positive semi-definite (and therefore Hermitian), and has trace 1. Conversely, by the spectral theorem, any such matrix has a decomposition of the form of equation 1, and corresponds to some ensemble of pure states.

The ensemble of pure states can be derived from a density matrix by looking at the eigendecomposition: by positive definiteness, we know that the eigenvalues are all real and positive; and since the matrix has trace 1, we know that the eigenvalues sum up to 1. Thus, the eigenvalues can be interpreted as probabilities, and the eigenvectors as the corresponding pure states.

We note that distinct ensembles of states could correspond to the same density matrix. For example, the ensembles $\{(\frac{1}{2}, |0\rangle), (\frac{1}{2}, |1\rangle)\}$ and $\{(\frac{1}{2}, |+\rangle), (\frac{1}{2}, |-\rangle)\}$ correspond to the same mixed state

$$\rho = \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{pmatrix} \tag{2}$$

We note that this happens when ρ has an eigenvalue of multiplicity greater than 1 (though not only then!).

Multipartite systems and the partial trace. If we have several quantum systems, the *joint state space* is the tensor product of the Hilbert spaces of the individual systems. For instance, if we have two systems associated with Hilbert spaces $\mathcal{X}$ and $\mathcal{Y}$, respectively, then the space of joint states of the two systems is $\mathcal{X} \otimes \mathcal{Y}$. Note that most states in the tensor product space cannot be factorized themselves as tensor products. Such states are called *entangled states*. States that can be factorized this way are called *product states*.

If we have a joint state $\rho_{\mathcal{X}\mathcal{Y}}$, then we can assign a state to a single system, say $\mathcal{X}$, by applying the *partial trace*:

$$\rho_{\mathcal{X}} = \mathrm{Tr}_{\mathcal{Y}}[\rho_{\mathcal{X}\mathcal{Y}}] = \sum_{i=1}^{d} (I \otimes \langle i|)\rho_{\mathcal{X}\mathcal{Y}}(I \otimes |i\rangle).$$

Purification ("The Church of the Larger Hilbert Space"). Any ensemble of states $\{(p_i, |\psi_i\rangle)\}_{i=1}^m$ over $\mathcal{X}$ can be represented as the partial trace of a pure state defined over a larger Hilbert space $\mathcal{X} \otimes \mathcal{Y}$. For example, the ensemble under consideration can be purified as

$$|\Psi\rangle = \sum_{i=1}^{m} \sqrt{p_i} \cdot |\psi_i\rangle \otimes |i\rangle$$

where $\{|i\rangle\}$ form a basis of the m-dimensional Hilbert space $\mathcal{Y}$. Indeed,

$$\sum_{i=1}^{m} (I \otimes \langle i|) |\Psi\rangle \langle\Psi| (I \otimes |i\rangle) = \sum_{i=1}^{m} p_i |\psi_i\rangle \langle\psi_i| = \rho,$$

the density matrix associated to the ensemble. Note, however, that this is but one of infinitely many purifications of the same ensemble of states. The following lemma states that any two such purifications are related by a unitary map applied to the purifying register.

Lemma 1. *For any two purifications $|\Psi_1\rangle, |\Psi_2\rangle \in \mathcal{X} \otimes \mathcal{Y}$ of the same ensemble of states over the state space $\mathcal{X}$, there is a unitary map $U : \mathcal{Y} \to \mathcal{Y}$ such that*

$$|\Psi_2\rangle = (I \otimes U) |\Psi_1\rangle$$

For example, the density matrix ρ in equation 2 can be purified in three ways as

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}}, \frac{|{+}{+}\rangle + |{-}{-}\rangle}{\sqrt{2}}, \text{ and } \frac{|00\rangle + |01\rangle + |10\rangle - |11\rangle}{2}$$

The first two of these are exactly the same state but the third can be transformed into the first (or the second) by applying the unitary map $I \otimes H$.

2.3 Entanglement and the maximally entangled state

We say that a *pure* state of a bipartite (or multipartite) system is *entangled* if it cannot be written as a tensor product of states of the individual systems:

$$|\psi\rangle_{\mathcal{AB}} \neq |\phi\rangle_{\mathcal{A}} \otimes |\chi\rangle_{\mathcal{B}}\,.$$

This definition extends to mixed states: a mixed state ρ is entangled if it can't be written as an ensemble of pure product states. (Unentangled mixed states are called "separable"; note that this does not necessarily mean product, as such states can still be classically correlated.)

An extremely useful state is the *maximally entangled state*. In fact, we are abusing terminology a bit: many states are maximally entangled, but we will use the term to refer to a *particular* bipartite state, on two systems $\mathcal{X}$ and $\mathcal{Y}$ of equal dimension d:

$$|\Phi\rangle = \frac{1}{\sqrt{d}} \sum_i |i\rangle_{\mathcal{X}} \otimes |i\rangle_{\mathcal{Y}}\,.$$

The special case where $d = 2$ is often called the *EPR pair* state

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}}\,.$$

Mathematically, this state is a useful object for "moving" operators between two systems. In particular, we have the identity

$$(M \otimes I)\,|\Phi\rangle = (I \otimes M^T)\,|\Phi\rangle\,,$$

where M is any square matrix. This identity is at the heart of *quantum teleportation*. Another way in which this state is useful is that it lets us express the "vectorization" of a matrix

$$M = \sum_{ij} M_{ij}\,|i\rangle\langle j| \mapsto \text{vectorize}(M) = \sum_{ij} M_{ij}\,|i\rangle \otimes |j\rangle\,.$$

It can be checked that

$$(M \otimes I)\,|\Phi\rangle = \frac{1}{\sqrt{d}} \sum_{ijk} M_{ij}(|i\rangle\langle j| \otimes I)(|k\rangle \otimes |k\rangle) \tag{3}$$

$$= \frac{1}{\sqrt{d}} \sum_{ij} M_{ij}\,|i\rangle \otimes |j\rangle \tag{4}$$

$$= \frac{1}{\sqrt{d}}\text{vectorize}(M). \tag{5}$$

This operation is often useful; it is the principle behind the Choi representation of quantum channels, which we will see later.

2.4 Quantum Computations and Quantum Channels

Most basically, quantum computation is performed via unitary matrices $U : \mathcal{X} \to \mathcal{X}$ where $U^\dagger U = \mathrm{Id}$. These map quantum states (unit vectors in $\mathcal{X}$) to other quantum states. A more general definition is that of a quantum channel:

Definition 2. *A quantum channel from a Hilbert space $\mathcal{X}$ to a Hilbert space $\mathcal{Y}$ is a **linear** map $\Phi : \mathcal{L}(\mathcal{X}) \to \mathcal{L}(\mathcal{Y})$ such that*

1. *Φ is **completely positive**: for every Hilbert space $\mathcal{Z}$, the map $\Phi \otimes \mathtt{Id}_{\mathcal{Z}}$ is positive; that is, for every $\rho \in \mathcal{P}(\mathcal{X} \otimes \mathcal{Z})$,*
$$(\Phi \otimes \mathtt{Id}_{\mathcal{Z}})\rho \in \mathcal{P}(\mathcal{Y} \otimes \mathcal{Z});$$
2. *Φ is **trace-preserving**: for every $\rho \in \mathcal{L}(\mathcal{X})$,*
$$\mathsf{Tr}_{\mathcal{Y}}(\Phi(\rho)) = \mathsf{Tr}_{\mathcal{X}}(\rho) .$$

While we define a channel as acting on any linear map, we will typically apply it to density matrices, i.e. $\rho \in \mathcal{S}(\mathcal{X})$.

Any quantum channel is a unitary on a larger Hilbert space. This is the content of Stinespring's dilation theorem, stated formally below.

Lemma 3 (Stinespring)**.** *For any quantum channel $T : S(\mathcal{X}_1) \to S(\mathcal{X}_2)$, there are Hilbert spaces $\mathcal{Y}_1$ and $\mathcal{Y}_2$ and a unitary map $U : \mathcal{X}_1 \otimes \mathcal{Y}_1 \to \mathcal{X}_2 \otimes \mathcal{Y}_2$ such that for any $\rho \in S(\mathcal{X}_1)$,*
$$T(\rho) = \mathrm{Tr}_{\mathcal{Y}_2}\left[U(\rho \otimes |0\rangle\langle 0|_{\mathcal{Y}_1})U^\dagger\right] .$$

2.5 Modeling classical information with quantum mechanics

In cryptography we usually imagine that we have some classical parties who are using quantum devices to perform a task.

- Can always model classical operations with quantum mechanics
- A deterministic classical state turns into a pure computational basis state.
- Classical *randomness* can be *simulated* using pure quantum states as well! Replace each uniformly random coin with a $|+\rangle$ state.
- Any deterministic classical computation corresponds to a unitary (acting on a possibly larger system). Concretely, if one has a classical boolean circuit, can convert it into a unitary by first converting into a classical *reversible* circuit, adding ancilla bits as necessary. Then each classical reversible gate automatically lifts to a unitary quantum gate.
- A randomized computation is just a deterministic computation that takes in a tape of random coins as an input. Often useful to represent this "coherently": convert the random coins to $|+\rangle$ states, and the computation to a unitary

2.6 Measurements

Most basically, given a system in a pure state $|\psi\rangle = \sum_j \alpha_j |j\rangle$ a *computational basis measurement* is a randomized process that outputs outcome j with probability $|\alpha_j|^2$, and leaves the system in the state $|j\rangle$.

More generally, a *von Neumann measurement* or *projective measurement* is specified by a collection of pairwise orthogonal projectors $\{\Pi_k\}$ such that $\sum_k \Pi_k = I$. An projector Π_k is a Hermitian matrix that satisfies $\Pi_k^2 = \Pi_k$. The pairwise orthogonality condition is that $\Pi_k \Pi_\ell = 0$ for any $k \neq \ell$.

Performing the measurement returns the outcome k with probability

$$\Pr[k] = \langle\psi| \Pi_k |\psi\rangle = \|\Pi_k |\psi\rangle\|^2,$$

and leaves the system in the state $\Pi_k |\psi\rangle / \|\Pi_k |\psi\rangle\|$. It is easy to see that the computational basis measurement is a special case of this, with one projector $\Pi_k = |k\rangle\langle k|$ for each basis element $|k\rangle$.

There is an even more general type of measurement called a *POVM measurement*. This is specified by a collection of PSD matrices $\{M_k\}$ such that $\sum_k M_k = I$. The measurement returns the outcome k with probability

$$\Pr[k] = \langle\psi| M_k |\psi\rangle = \mathrm{Tr}[M_k |\psi\rangle\langle\psi|]$$

and leaves the system in the *mixed* state

$$\rho = \frac{\sqrt{M_k} |\psi\rangle\langle\psi| \sqrt{M_k}}{\mathrm{Tr}[M_k |\psi\rangle\langle\psi|]}.$$

POVM measurements turn out to be the most general type of measurement. Moreover, just like with channels and unitaries, it turns out that every POVM measurement is equivalent to a projective measurement on the system after adjoining an ancilla register. (POVM : projective measurement :: Channels : Unitaries.) This is called the *Naimark dilation theorem*.

All these formulas can be generalized to mixed state inputs. The most useful one to remember is the probability for outcome k in a POVM measurement of $\{M_k\}$ on state ρ is

$$\Pr[k] = \mathrm{Tr}[M_k \rho].$$

A binary measuement $\{\Pi_0, \Pi_1\}$ can be translated into an observable $O = \Pi_0 - \Pi_1$ which is just a Hermitian matrix $O^\dagger = O$ and $O^2 = I$. The expected value of the measurement can then be written as

$$\mathbb{E}\,(-1)^b = \Pr[0] - \Pr[1] = \langle\psi| O |\psi\rangle$$

2.7 The Pauli matrices

For working with qubits, an extremely useful set of matrices is the Paulis.

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

(To remember the Y matrix, a useful mnemonic is "minus i flies high.")

These are all binary observables, and therefore also unitaries. So they can be viewed as describing both measurements as well as transformations of quantum states.

The eigenstates of X and Z are very common, and denoted $|0\rangle, |1\rangle, |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$.

A related matrix that is useful (and which is also a binary observable) is the Hadamard matrix

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

This has the useful property of mapping X eigenstates to corresponding eigenstates of Z, and vice versa, which follows from the relation

$$HX = ZH.$$

3 An example protocol: Wiesner's Quantum Money

In 1970, Wiesner came up with the very first protocol to use quantum information in an interesting way (thought it was only published in 1983). This was his protocol for *quantum money*.

The idea is the following: a classical banknote can always be forged *in principle* (with a good enough scanner and printer, the right paper, good enough ink, etc.). This is essentially because classical information can be copied without disturbance. But quantum information is different: measurement will in general disturb a quantum state. Could a banknote consisting of quantum particles be physically *impossible* to forge without damaging it?

Wiesner's scheme was as follows. The mint generates banknotes, that consist of n qubits each. To generate a fresh banknote, the bank chooses a random *serial number* $s \in \{0,1\}^{2n}$, and a pair of random strings $a, b \in \{0,1\}^{2n}$. It then creates the state

$$|\psi_s\rangle = H^{\otimes a} |b\rangle .$$

This state is a product state. The ith qubit is in the state

- $|0\rangle$ if $a_i, b_i = 00$,
- $|1\rangle$ if $a_i, b_i = 01$,
- $|+\rangle$ if $a_i, b_i = 10$,
- $|-\rangle$ if $a_i, b_i = 11$.

The bank writes down (s, a, b) in its secret ledger, and then publishes the pair $(s, |\psi_s\rangle)$ as the banknote.

Now, suppose I want to use a quantum banknote to buy something. The banknote will be sent to the bank for verification. The bank will look up the serial number s in the secret ledger, and then measure each qubit in the X or Z basis according to a, and check that the outcomes match b. If the note was valid, this process does not damage the state at all, and the bank accepts. If the note was far from a valid note, the bank will reject with decent probability. The probability that the bank accepts a state $|\phi\rangle$ for a serial number s is given by

$$\Pr[accept] = |\langle\psi_s|\phi\rangle|^2.$$

Wiesner claimed that this scheme was *secure*. What this means precisely will be specified in future lectures, but at a minimum, it means that an adversary should have a low chance of being able to generate two banknotes that both pass the bank's verification procedure for the same serial number. Why is this true?

Heuristically, the idea is that the adversary cannot learn the state of the banknote to copy it, because they have no idea which basis each qubit is in. If they accidentally measure a $|0/1\rangle$ qubit in the $|\pm\rangle$ basis, this would return a uniformly random outcome, and destroy the state. With n qubits, the chance of guessing all the bases correctly should surely be exponentially small in n...

How do we make this idea rigorous? We will build towards this next time.

References

[Wat18] John Watrous. *The Theory of Quantum Information.* Cambridge University Press, 2018.