Week 9 : Quantum Cryptography

Cryptography is the study of mathematical techniques for securing digital information, systems, and distributed computations against adversarial attacks.

Quantum cryptography is the science of exploiting quantum mechanical properties in order to carry out cryptographic tasks. One such area of application is the Key Distribution problem, in the symmetric key setting, where two communicating parties must share a secret key before starting communications. In the classical setting this is not possible unless the parties have a secure communcation channel, however, quantum key distribution offers a solution.

1 Classical Cryptography

Before studying quantum cryptography we must familiarise ourselves with the ideas of cryptography in general.

In any communication scenario we have two parties – the sender and the reciever – trying to communicate over a insecure channel. These parties are typically named Alice and Bob in cryptographic literature. The communication channel being insecure, is susceptible to eavesdropping by a third character, Eve. Thus, Alice and Bob are presented with the problem of communicating securely over an insecure channel. Since the aim of this text to discuss quantum key distribution we shall be working in symmetric key setting i.e. the Alice and Bob use a secret key which has been shared by them in advance.

The problem is solved by the use of an *encryption scheme* such that provided both parties know the secret key one of them can *encrypt* the message and the other can *decrypt* the message.

1.1 Encryption Schemes

An encryption scheme is defined by three algorithms, $(\mathrm{Gen}, \mathrm{Enc}, \mathrm{Dec})$ as well as a finite, non-empty message space $\mathcal{M}$. The key-generation algorithm Gen is a probabilistic algorithm that outputs a key k chosen according to some distribution. We denote by $\mathcal{K}$ the (finite) key space, i.e., the set of all possible keys that can be output by Gen. The encryption algorithm Enc takes as input a key $k \in \mathcal{K}$ and a message $m \in \mathcal{M}$, and outputs a ciphertext c. The decryption algorithm Dec takes as input a key $k \in \mathcal{K}$ and a ciphertext $c \in \mathcal{C}$ and outputs a

message $m \in \mathcal{M}$. We assume perfect correctness, meaning that for all $k \in \mathcal{K}$, $m \in \mathcal{M}$, and any ciphertext c output by $\text{Enc}_k(m)$ (shorthand for $\text{Enc}(k, n)$), it holds that $\text{Dec}_k(c) = m$ (defined analogous to that of $\text{Enc}_k(m)$) with probability 1.

1.2 Perfect Secrecy

Now that we have a definition of an encryption scheme, it is only natural to ask how secure it is.

One such guarantee of security is provided by the notion of perfect secrecy. One can safely say that an encryption scheme is secure if an adversary can gain no extra knowledge about the message sent just by observing the ciphertext.

Formally:

Definition. An encryption scheme (Gen, Enc, Dec) with message space $\mathcal{M}$ is perfectly secret if for every probability distribution over $\mathcal{M}$, every message $m \in \mathcal{M}$, and every ciphertext $c \in \mathcal{C}$ for which $\Pr[C = c] > 0$:

$$\Pr[M = m | C = c] = \Pr[M = m].$$

Thus, perfect secrecy guarantees information theoretic security – the system cannot be broken even if the adversary has unlimited computational power.

1.3 One Time Pad

Now that we have defined both, an encryption scheme and the notion define of perfect secrecy, let us look at one such construction that satisfies both criteria – the one time pad:

- Gen: the key generation algorithm chooses a key form $\mathcal{K} = \{0,1\}^\ell$ according to the uniform distribution.
- Enc: given a key $k \in \{0,1\}^\ell$ and a message $m \in \{0,1\}^\ell$, the encryption algorithm outputs the ciphertext $c = k \oplus m$.
- Dec: given a key $k \in \{0,1\}^\ell$ and ciphertext $c \in \{0,1\}^\ell$, the decryption algorithm outputs the message $m = k \oplus c$.

One would think that having a perfectly secret encryption scheme would entirely solve the confidentiality problem in cryptography. However, perfectly secret schemes have a severe shortcoming – the key used to encrypt a message must be at least as long as the message. This is a rather tricky requirement; if parties were able to secure exchange such a key they might as well use the same method to communicate the message. This is where quantum key distribution might help us.

(Note, there are in fact other issues which make the one time pad less than ideal to use in a practical scenario, such as requiring truly random keys as opposed to pseudo random keys. However, these issues aren't the primary concern of this text.)

2 Quantum Key Distribution

Quantum key distribution is a secure communication method which involves using quantum mechanical properties in order to let two parties to exchange a random secret key known only to them.

There are some fundamental properties of quantum mechanics which are critical to the working of quantum key distribution. Let us compare the classical and the quantum cases. When Alice and Bob are communicating using classical bits, Eve can copy arbitrary positions of the encrypted bit stream and store them for later analysis, moreover, her eavesdropping cannot be detected. However, when Alice and Bob are communicating using qubits Eve cannot make copies of the qubit stream as a consequence of the no-cloning theorem, in fact if she measured any of the qubits, the qubit stream would be disturbed in manner which can later be detected. Thus, qubits posses some qualities which are very appealing to cryptographers.

Over the years, there have been a few of quantum key distribution protocols which have been designed. We shall be discussing four of them – the BB84, E91, BB92 and EPR protocols.

2.1 The BB84 Protocol

The BB84 protocol was the first quantum key distribution protocol which was introduced by Charles Bennet and Gilles Brassard in 1984.

In the BB84 scheme, Alice wishes to send a private key to Bob via a quantum channel. She begins with two random classical, n bit long bit strings, a and b. She then encodes these two strings as a tensor product of n qubits:

$$|\psi\rangle = \bigotimes_{i=1}^{n} |\psi_{a_i b_i}\rangle,$$

where a_i and b_i are the i-th bits of a and b respectively. Therefore, $a_i b_i$ can correspond to 00, 01, 10, and 11 giving us one of the following four qubit states:

$$|\psi_{00}\rangle = |0\rangle,$$

$$|\psi_{10}\rangle = |1\rangle,$$

$$|\psi_{01}\rangle = |+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle,$$

$$|\psi_{11}\rangle = |-\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle.$$

Note that the bit b_i is what decides which basis a_i is encoded in (either in the computational basis or the Hadamard basis). Thus, the knowledge of b is required to distinguish all the qubits with total accuracy, since they are in states which are not mutually orthogonal.

Alice transmits $|\psi\rangle$ to Bob over an insecure and authenticated quantum channel. Bob receives a state $\mathcal{E}(\rho) = \mathcal{E}(|\psi\rangle\langle\psi|)$, where $\mathcal{E}$ represents both the effects of noise in the channel and eavesdropping by Eve. After Bob receives the string of qubits, all three parties, namely Alice, Bob and Eve, have their own states. However, since only Alice knows b, it makes it virtually impossible for either Bob or Eve to distinguish the states of the qubits since both of them guess which basis Alice used to encode any particular bit. As a consequence of the no-cloning theorem Eve cannot have a copy of the qubits which Alice sent to Bob, unless she measured them. Her measurements, however, risk disturbing a particular qubit with probability $\frac{1}{2}$ if she guesses the wrong basis. (Say Alice sends the bit $|+\rangle$ to Bob, however Bob chooses the computational basis where $|+\rangle$ corresponds to the superposition $\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$. Therefore, upon measurement Bob will only get the correct bit with probability $\frac{1}{2}$.)

Bob then generates a random n bit long string b' and then measures the string he has received from Alice, a'. At this point, Bob announces publicly that he has received Alice's transmission. Alice then knows she can now safely announce b. Bob communicates over a public channel with Alice to determine which b_i and b'_i are not equal. Both Alice and Bob now discard the qubits in a and a' where b and b' do not match.

From the remaining k bits where both Alice and Bob measured in the same basis, Alice randomly chooses $k/2$ bits and discloses her choices over the public channel. Both Alice and Bob announce these bits publicly and run a check to see whether more than a certain number of them agree. If this check passes, Alice and Bob proceed to use information reconciliation and privacy amplification techniques to create some number of shared secret keys. Otherwise, they must restart the process.

2.2 The E91 Protocol

The protocol was given by Artur Ekart in 1991.

The protocol is dependant on Alice and Bob having a entangled pairs of photons. The source of these photons is immaterial (even Eve could have made them), only that they are entangled, and that Alice and Bob have one photon from each pair.

There are two properties of entangled photons which are critical to the correct working of the protocol. Entangled photons always have the same polarisation when measured by either Alice or Bob, even if the polarisation of distinct pairs are randomly distributed. This correlation holds true for pairs with orthogonal polarisation as well. Second, any attempt at eavesdropping by Eve destroys these correlations.

Just like the BB84 protocol Alice and Bob privately measure the qubits before attempting to detect Eve's attempts at eavesdropping. Alice measures her photons using the some bases from the set $\{T_0, T_{\frac{\pi}{8}}, T_{\frac{\pi}{4}}\}$ and Bob measures his photons using some bases from the set $\{T_0, T_{\frac{\pi}{8}}, T_{\frac{-\pi}{8}}\}$ (where T_θ represents the computational basis rotated by θ). The choices of bases are secret till the measurements are done, after which the choices of bases are compared. The photons for which Alices' and Bob's choice of bases disagree are discarded.

In keeping with Bell's Theorem maximally entangled photons would behave differently from those pairs of photons which as a result of Eve's eavesdropping were no longer maximally entangled. If successful, the photons from the first group can be used to generate a key due to their anti-aligned nature.

2.3 The B92 Protocol

In the BB84 protocol we saw that Alice used to distinct orthogonal bases. It turns out that the use of two different bases is redundant, provided we use a smarter measurement technique.

Charles Bennet gave this protocol in 1992.

The main idea used in B92 is that Alice uses only one non-orthogonal basis. One of way doing this is choosing one vector each of the computational basis and the Hadamard basis. The example we shall be working with is $|0\rangle$ and $|+\rangle$. Observables have an orthogonal basis of eigenvectors. Therefore, there may be no observable with the basis of eigenvectors we have chosen. In other words no experiment can be set up to distinguish the non-orthogonal states of our basis.

Alice wishes to send Bob an n bit secret key over an insecure, authenticated quantum channel. She generates an n bit random string a. The i-th bit of a can be either be 0 or 1 and is transmitted $|0\rangle$ or $|+\rangle$ respectively.

After Bob receives Alice's qubit stream, he generates an n bit random string b. If the i-th bit of b is 0 Bob measures the i-th qubit in the computational basis, else the Hadamard basis. There are a number cases one can consider here. If Bob uses the computational basis and observes a $|1\rangle$, he is certain that Alice must have sent a $|+\rangle$, else he would have observed a $|0\rangle$. However, if Bob observes a $|0\rangle$, then it is uncertain whether Alice sent him a $|0\rangle$ or a $|+\rangle$ vector. The case when Bob chooses the Hadamard basis to measure the qubit is similar. Thus, for each of the two bases that Bob could have used to measure, there are two types of results. For half of those four results, the bit sent is certain. Bob must discard these uncertain bits.

Bob publicly tells Alice which bits were uncertain, and they both omit them. At this point they both know which bits are secret. They publicly compare half of the secrets bits and if more than a tolerable number are

Exercises

Theory Questions

1. Prove that one time pad is perfectly secure.

2. Prove that for a perfectly secret scheme, the key length is at least as long as the message length.

3. Alice and Bob are trying to exchange a key using the BB84 protocol. Eve consistently eavesdrops every qubit being sent from Alice to Bob. How frequently will Bob's bits agree with Alice's?

4. Verify that the basis vectors used by Alice in the B92 protocol are orthogonal.

5. If computer scientists come up a cheap and computationally efficient quantum key distribution algorithm, will that be the end of cryptography?