Quantum Cryptography

Week 8

Introduction

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.
    - e.g Quantum key distribution

Classical Cryptography

Classical Cryptography

- Consists of two parties (Alice and Bob) trying to communicate securely over insecure channel.
- Eve, a third party is trying to spy on Alice and Bob.
- Alice and Bob use symmetric key cryptographic protocols by sharing a key before hand.
    - e.g. One time pad

Encryption Scheme

- Consists of three algorithms,

  Gen Generates a key k, which shared by both parties beforehand. $k \leftarrow \textsf{Gen}$.

  Enc Accepts key k, and plaintext m to give ciphertext c. $\textsf{Enc}_k(m) = c$.

  Dec Accepts key k, and ciphertext c to give plaintext p. $\textsf{Dec}_k(c) = m$.

- We assume *correctness* of cipher, i.e. for any key k and message m, $\textsf{Dec}_k \textsf{Enc}_k(m) = m$.

Perfect Secrecy

- It is necessary to have a definition of how secure a scheme is.

Definition
An encryption scheme $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ 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 $\Pr[C = c] > 0$:

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

- Perfect secrecy guarantees that the system cannot be broken even if the adversary has unlimited computational power. Why?

One Time Pad

- Example of a perfectly secret scheme.

  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 $m = k \oplus c$.

- Key sharing is problematic. Key must be at least as long as message!
- Quantum key distribution is a solution!

Quantum Key Distribution

Quantum Key Distribution

- 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.
- Quantum properties lend themselves naturally to key distribution problem:
  - Eve can't copy qubits. No-cloning theorem!
  - Eve eavesdropping can detected later.
- e.g BB84, BB92, E91

BB84

- First Quantum Key Distribution protocol.
- Given by Charles Bennet and Gilles Brassard in 1984.
- The protocol works in the following way,
  - Alice randomly generates key bit, and sends to it to Bob, encoded randomly in the computational or the Hadamard basis. Bob guesses which basis and measures qubit. If Bob guessed correctly the bits match.
  - Alice and Bob compare choice of bases, and discard bits which they disagreed on. Half the bits are then compared, and if many of them don't match then, then this is chalked off as a result of Eve's mischief and the process is restarted.

B92

- Given by Charles Bennet in 1992.
- It is improvement over the BB84 protocol.
- Alice uses a single non-orthogonal basis, instead of two orthogonal bases. The secruity relies on the fact that non-orthogonal states can’t be distinguished reliably.
- The algorithm proceeds in a manner similar to the BB84 protocol. A detailed description has been omitted. Readers may refer to handout.

E91

- Given by Artur Ekart in 1991.
- Relies on entanglement to provide security.
- Alice and Bob get entangled qubits from some source. The measure theme from fixed set of bases, by choosing a basis randomly. Alice and Bob declare their choice of bases, and discard the qubits where they disagreed. Now, in keeping with Bell's inequality, these qubits should collapse to the same value, *unless* they have been tampered by Eve. Alice and Bob check half the bits, and if many of them disagree the process is restarted.