CS 599 P1: Introduction to Quantum Computation Boston University, Fall 2025
Instructor: Alexander Poremba

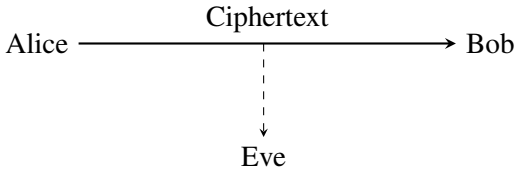
LECTURE # 23: QUANTUM CRYPTOGRAPHY

In this lecture, we shift our focus from protecting quantum information against noise to protecting *classical information* against an adversary. We begin by reviewing the notion of secret-key cryptography and the celebrated one-time pad, a cryptosystem which achieves *perfect information-theoretic security*. We then address a fundamental limitation of such schemes: the requirement that communicating parties must already share a secret key. This leads us naturally to the problem of *key exchange* and, ultimately, to *Quantum Key Distribution (QKD)*, which leverages quantum mechanics to establish shared secret keys without relying on computational assumptions.

1 A perfectly secure cryptosystem

We begin with the standard setting of *secret-key cryptography*. Two parties, traditionally called Alice and Bob, wish to communicate a message over an insecure channel. An adversary, Eve, has full access to the communication channel and may intercept all transmitted data.

The communication model. Alice wishes to send a message $m \in \{0,1\}^n$ to Bob. Alice and Bob initially share a secret key $k \in \{0,1\}^n$, unknown to Eve. The goal is to design an encryption scheme such that Bob can recover m from the ciphertext, while Eve learns essentially nothing about m.



This raises a fundamental question:

> *Can Alice send a message to Bob in such a way that Eve learns virtually nothing about the message?*

The one-time pad. The answer is affirmative, provided Alice and Bob share a secret key of sufficient length. The classical *one-time pad* is defined as follows.

- **Key:** A uniformly random key $k \in \{0,1\}^n$
- **Encryption:** $c = m \oplus k$
- **Decryption:** $m = c \oplus k$

Correctness follows immediately from the identity $(m \oplus k) \oplus k = m$.

Perfect security. The one-time pad enjoys a remarkably strong security guarantee.

Perfect secrecy of the one-time pad

For every message $m \in \{0,1\}^n$ and every ciphertext $c \in \{0,1\}^n$,

$$\Pr[m \mid c] = \Pr[m].$$

That is, observing the ciphertext gives Eve no information whatsoever about the message.

Proof. For any fixed message m and ciphertext c, there exists a *unique* key $k = m \oplus c$ that produces c. Since k is uniformly random over $\{0,1\}^n$, all messages are equally likely given c. □

The danger of using the same key twice. The perfect security of the one-time pad hinges crucially on the fact that the key is used only once. If Alice encrypts two messages m_1, m_2 using the same key k, Eve observes

$$c_1 \oplus c_2 = m_1 \oplus m_2,$$

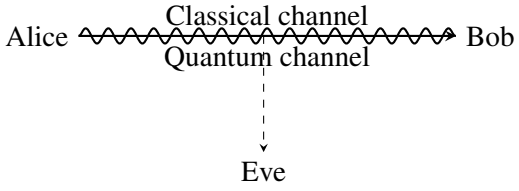
which may leak substantial information about the messages.

The key distribution problem. The one-time pad shifts the cryptographic challenge to the problem of *key exchange*: How can Alice and Bob establish a shared secret key in the first place?

Over a purely classical public channel, key exchange necessarily relies on *computational assumptions*. For example, the Diffie–Hellman protocol assumes the hardness of the discrete logarithm problem. If these assumptions fail (e.g. due to quantum algorithms), security collapses.

2 Quantum Key Distribution

Quantum Key Distribution (QKD) resolves the key distribution problem by exploiting fundamental principles of quantum mechanics. In addition to a public classical channel, Alice and Bob now have access to a *quantum channel* over which quantum states can be transmitted.



In practice, a quantum channel may consist of single photons sent through an optical fiber or free space, with information encoded in polarization or phase.

What QKD achieves. A QKD protocol allows Alice and Bob to establish a shared secret key such that:

- Any eavesdropping attempt by Eve introduces detectable disturbances.
- Security is information-theoretic and does not rely on computational hardness.
- The only classical assumption required is an *authenticated* classical channel.

2.1 The BB84 protocol

The first and most famous QKD protocol is BB84, introduced by Bennett and Brassard in 1984. It is based on the idea of *conjugate coding*.

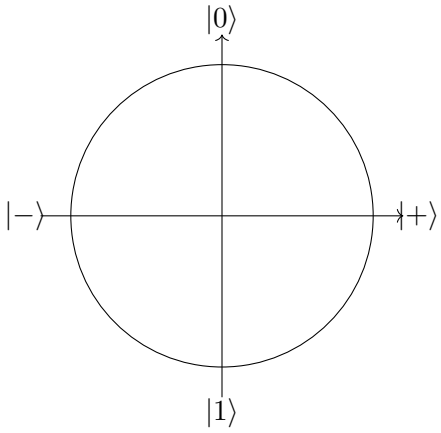
Conjugate bases. Let $x \in \{0,1\}$ and $\theta \in \{0,1\}$. We define the encoding

$$|\psi_{x,\theta}\rangle := H^\theta |x\rangle .$$

This yields four possible quantum states:

$$|0\rangle , \quad |1\rangle , \quad |+\rangle = H|0\rangle , \quad |-\rangle = H|1\rangle .$$

These states form two incompatible measurement bases indexed by θ.



Measuring a state prepared in one basis using the other basis yields a uniformly random outcome.

The BB84 Protocol (m qubits)

1. Alice samples random strings $x, \theta \in \{0,1\}^m$.
2. Alice prepares the state
$$|\psi\rangle = \bigotimes_{i=1}^{m} H^{\theta_i} |x_i\rangle$$
and sends it to Bob over the quantum channel.
3. Bob chooses a random measurement basis $\theta'_i \in \{0,1\}$ for each qubit and measures.
4. Alice and Bob publicly announce θ and θ'.
5. They keep only positions where $\theta_i = \theta'_i$.
6. The remaining bits form a shared raw key.

2.2 Example

We now illustrate the BB84 protocol with a concrete example. Let $m = 8$ and suppose Alice samples the random strings

$$x = 01110100, \qquad \theta = 11010001.$$

Alice prepares the product state

$$\bigotimes_{i=1}^{8} H^{\theta_i} |x_i\rangle$$

and sends the eight qubits to Bob over the quantum channel.

Bob independently chooses a random measurement basis string $\theta' \in \{0,1\}^8$ and measures the i-th qubit in the computational basis if $\theta'_i = 0$ and in the Hadamard basis if $\theta'_i = 1$. One possible choice of θ' and the corresponding measurement outcomes is shown in the table below.

i	1	2	3	4	5	6	7	8
x_i	0	1	1	1	0	1	0	0
θ_i	1	1	0	1	0	0	0	1
θ'_i	0	1	0	0	0	1	0	1
Bob's outcome	?	1	1	?	0	?	0	0

After all measurements are completed, Alice and Bob publicly announce their basis choices θ and θ'. They *keep only those positions* i for which $\theta_i = \theta'_i$, since in these positions Bob measured in the correct basis and therefore recovers Alice's bit with certainty. All other positions are discarded.

In this example, the matching positions are

$$i \in \{2, 3, 5, 7, 8\}.$$

The corresponding bits form the shared raw key

$$(1, 1, 0, 0, 0).$$

Crucially, any attempt by an eavesdropper Eve to measure the quantum states would introduce detectable errors in these correlations, allowing Alice and Bob to estimate Eve's information and abort the protocol if necessary.