PHYSICS DEPARTMENT
IIT JODHPUR
-Prof. V. Narayanan

Quantum key Distribution Using Arduino Board

-Avinash Kumar

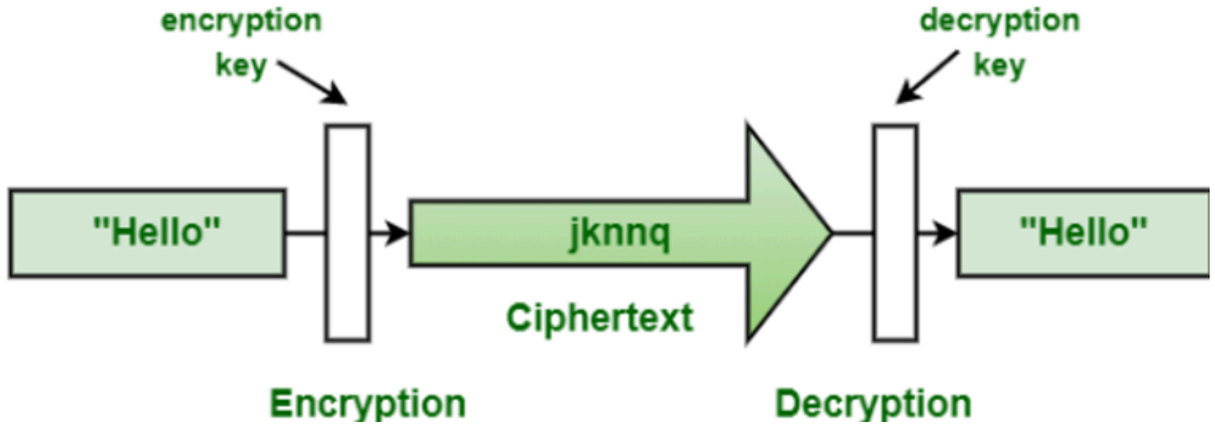
Table of Contents

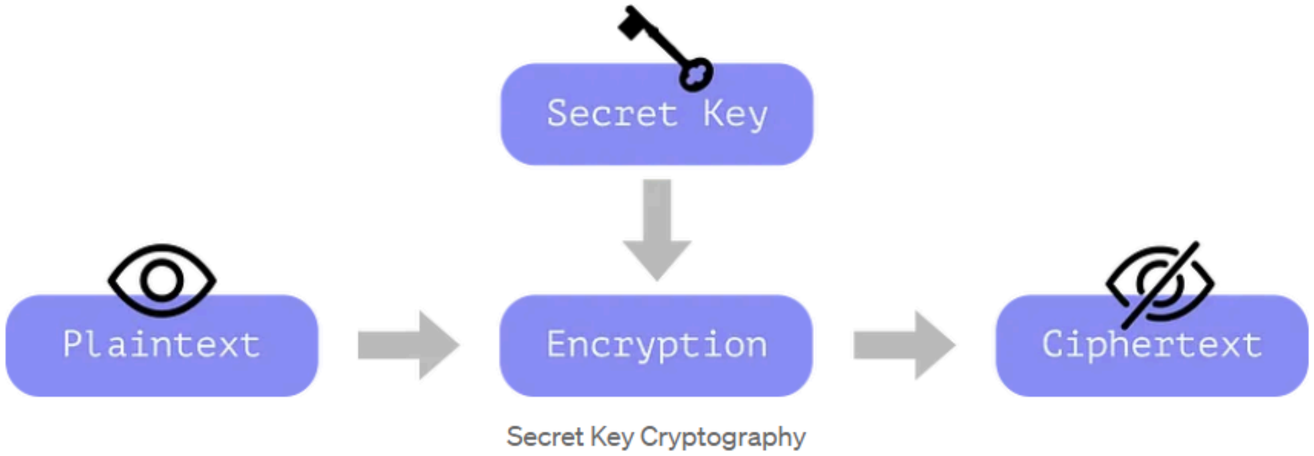
Introduction

Cryptography

It is the practice and study of techniques for secure communication by constructing and analyzing protocols that prevent third parties or the public from reading private messages.

Basic Idea

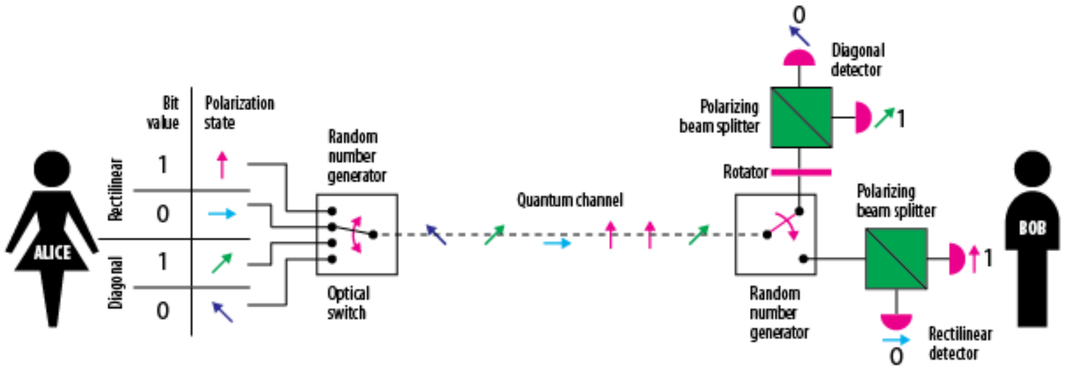

encryption
key
decryption
key
"Hello"
jknnq
Ciphertext
"Hello"
Encryption
Decryption


Secret Key
Plaintext
Encryption
Ciphertext
Secret Key Cryptography

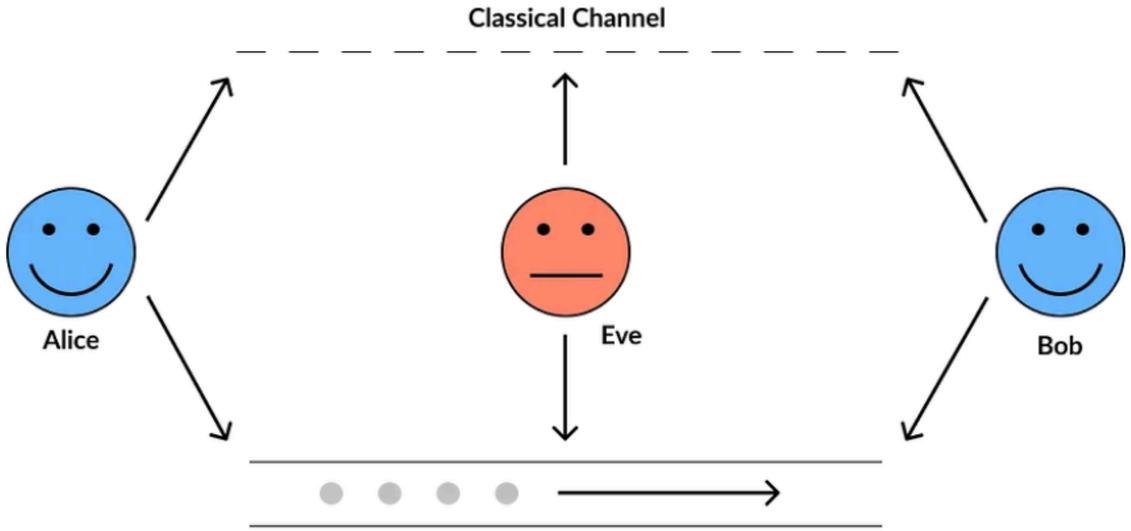
History of Cryptography

- Caeser Cipher
- Vigenere cipher
- Quantum cryptography

Quantum Cryptography



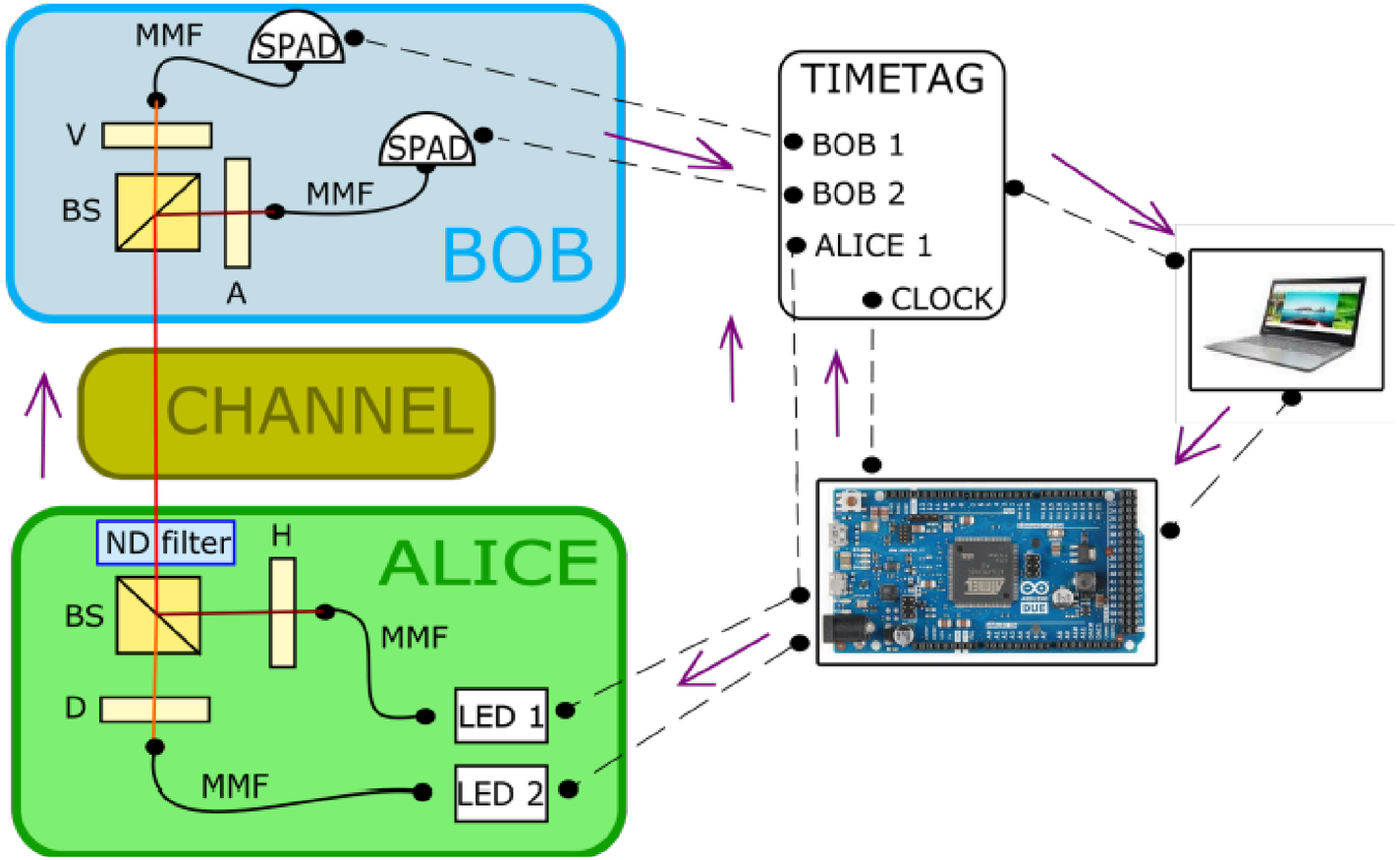
Quantum transmission & detection	ALICE sends photons	↖	↗	→	↑	↑	↗	↖	↑
	ALICE's random bits	0	1	0	1	1	1	0	1
	BOB's detection events	↑	↗	↖	↑	↗	↗	↖	↖
	BOB's detected bit values	1	1	0	1	1	1	0	0
Public discussion (i.e., sifting)	BOB tells ALICE the basis choices he made	Rect	Diag	Diag	Rect	Diag	Diag	Diag	Diag
	ALICE tells BOB which bits to keep		✔		✔		✔	✔	
	ALICE and BOB's shared sifted key	–	1	–	1	–	1	0	–



General representation of a QKD setup

- Experiment Setup

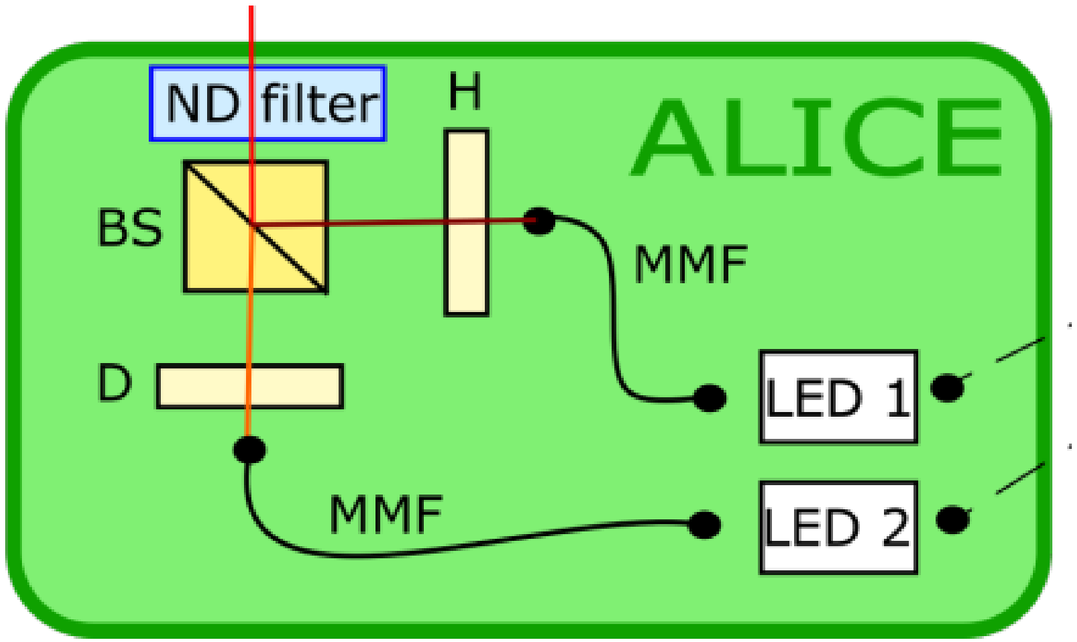
Setup



- LED-light emitting diode
- MMF-multi-mode optical fibre
- BS-beam splitter
- ND filter-set of neutral-density filter
- SPAD-single photons avalanche diode detector
- H(D)-horizontal(diagonal) polarization state preparation
- A(V)-antidiagonal(vertical) polarization state measurement

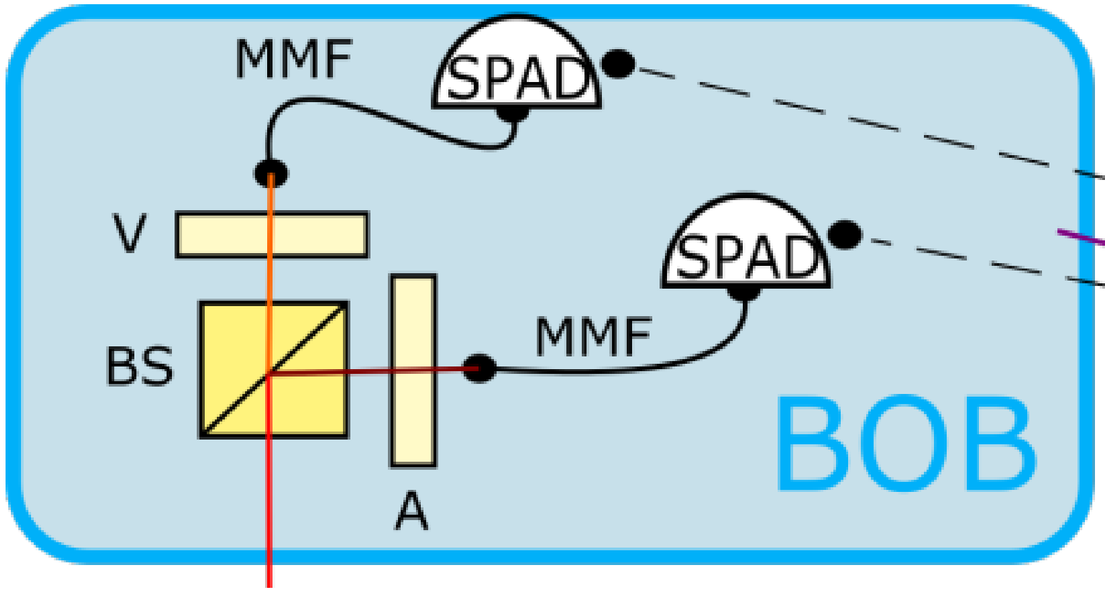
Transmittor

- **Light source** : OSRAM 850 nm light emitting diode(LEDs)
- **Spectral bandwidth**: 30 nm (FWHM)
- **Rise and fall time**: 12 ns
- **Pulse duration**: 24 ns
- **Light coupling**: MMF and FLS
- **Collimation**: FLS
- **Polarization**:Linear polarizer
- **Beam combination**: Balanced non-polarizing beam splitter
- **Attenuation**:ND filter
- **Spectral filtering**:Optical spectral filter to make LED's spectra indistinguishable

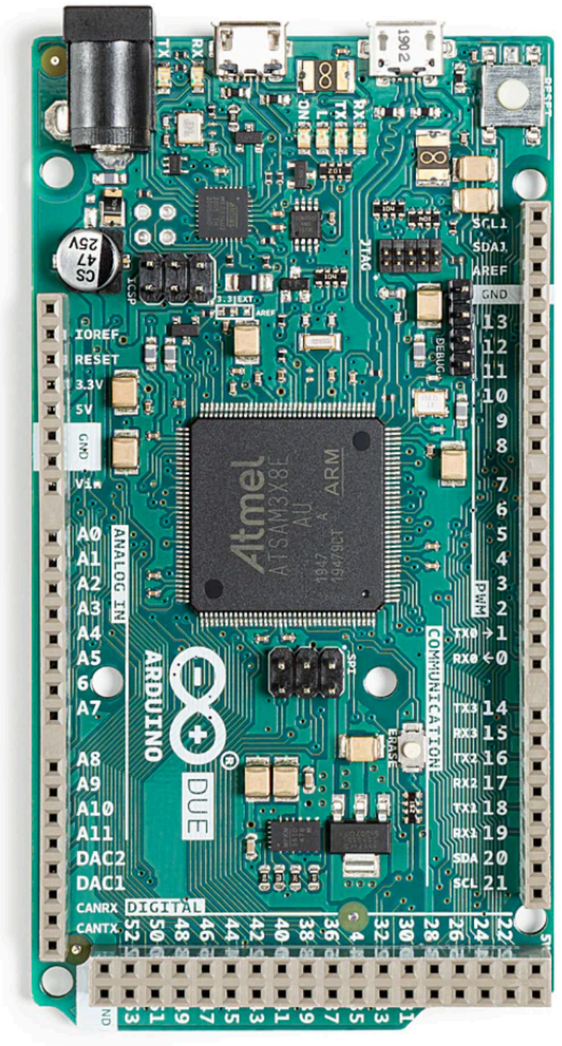


Receiver

- **Beam splitting**: Balanced non-polarizing beam splitter
- **Polarization analysis**:Two linear polarizer set to project onto antidiagonal and vertical linear polarization states
- **Losses**: 50% loss due to the BS
- **Photon detection**: SPADs from excelitas
- **Detection mechanism**: Avalanche current generation
- **Dead time** : 23 ns
- **Photon Detection efficiency**:56%
- **Dark count rate** : DC1= (53 ± 1) Hz, DC2= (77 ± 1) Hz
- **Dark count causes:** Thermal noise
- **Impact on bit error rate**: Dark counts increase the bit error rate



Arduino Due



Main Features

32-bit ARM core

Based on the ARM® Cortex®-M3 processor, this 32-bit microcontroller has 84 MHz clock and 96kb of SRAM.

54 digital pins

The Due has 54 digital pins, 12 of which support PWM (Pulse Width Modulation).

CAN support

The Due comes with two CAN (Controller Area Network) buses.

Analog pins

The Due has 12 analog input pins, and 2 DAC pins.

Keyboard / Mouse support

Use the Due as USB host for peripherals such as mice connected to the SerialUSB port.

Battery Connector

The Arduino Due features a barrel plug connector, that works great with a standard 9V battery.

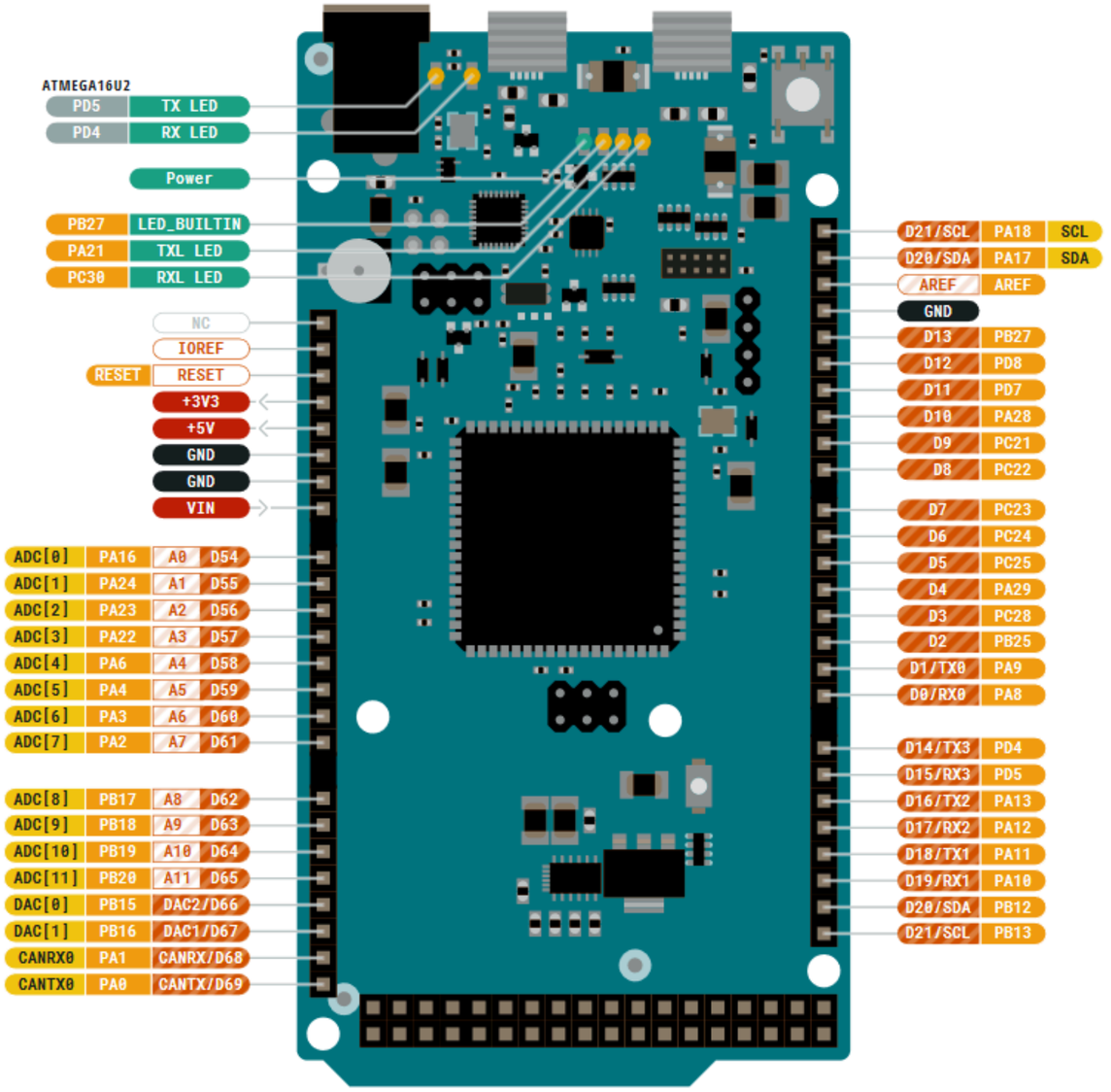
PIN CONFIGURATION

Pin Layout

Arduino Due's pin layout is designed for ease of use and understanding. Different types of pins are color-coded for quick identification

Types of PIN

- Digital Pins: Used for digital input or output.
- Analog Pins: Enable analog input for sensors.
- PWM Pins: Facilitate pulse-width modulation for precise control.
- DAC Pins: Used to give analog output.
- Each pin has specific functionalities, offering a wide range of options for connecting sensors, actuators, and other components.



Role of Arduino

THE ARDUINO CONTROLS THE EXPERIMENT BY GENERATING A CLOCK SIGNAL, PRODUCING RANDOM NUMBERS, AND SYNCHRONIZING THE SIGNALS.

- **CLOCK SIGNAL**: THE ARDUINO GENERATES A SQUARE WAVE SIGNAL THAT DEFINES THE TIME WINDOW FOR EACH BIT. THIS ENSURES THAT ALICE AND BOB ARE BOTH SENDING AND RECEIVING BITS AT THE SAME TIME.
- **RANDOM NUMBERS**: THE ARDUINO'S HARDWARE RANDOM NUMBER GENERATOR (HRNG) GENERATES A RANDOM SEQUENCE OF 0S AND 1S. THIS SEQUENCE IS USED TO DETERMINE WHICH LED TO TURN ON, WHICH CORRESPONDS TO WHICH BIT TO SEND.
- **SIGNAL SYNCHRONIZATION**: THE ARDUINO ENSURES THAT ALL OF THE SIGNALS ARE SYNCHRONIZED BY USING COAXIAL CABLES OF DIFFERENT LENGTHS. THIS IS IMPORTANT BECAUSE ALICE AND BOB CANNOT SHARE THE SAME CLOCK, SO THEY NEED TO SYNCHRONIZE THEIR CLOCKS IN ORDER TO COMMUNICATE EFFECTIVELY.

THE ARDUINO ALSO MONITORS THE SIGNALS FROM THE SPADS (SINGLE-PHOTON AVALANCHE DIODES) AT BOB'S SIDE. THESE SIGNALS INDICATE WHETHER OR NOT A PHOTON WAS DETECTED. THIS INFORMATION IS USED TO GENERATE THE RAW KEY

- B92 Protocol

Steps of B92 protocol:-

- Alice generates a random sequence of 0s and 1s
- For each bit, Alice randomly choose one of two polarization states for a photon (0 or 45 degree) and prepares the photon accordingly.
- Alice sends the stream of photon to Bob over a quantum channel.
- Bob randomly selects a basis(rectilinear or diagonal) for measuring each incoming photon.
- if Bob detects a photon, he determines its polarization state and the corresponding bit value. If he doesn't detect a photon , he discards that bit.
- Alice and Bob publicly compare a random sample of the bits to ensure there are no eavesdroppers. If errors are detected, the key is discarded and the process is repeated

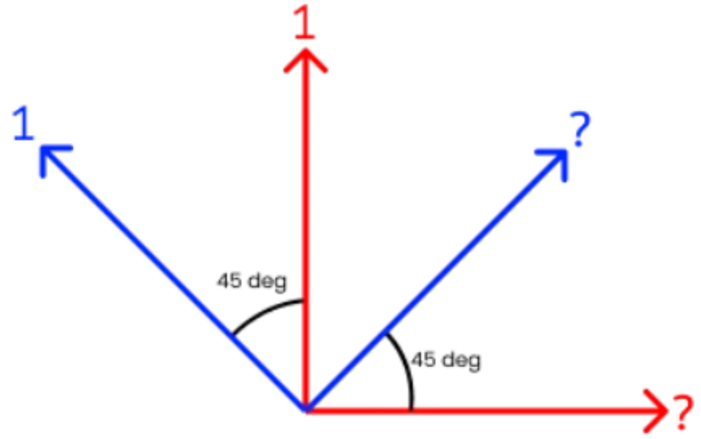
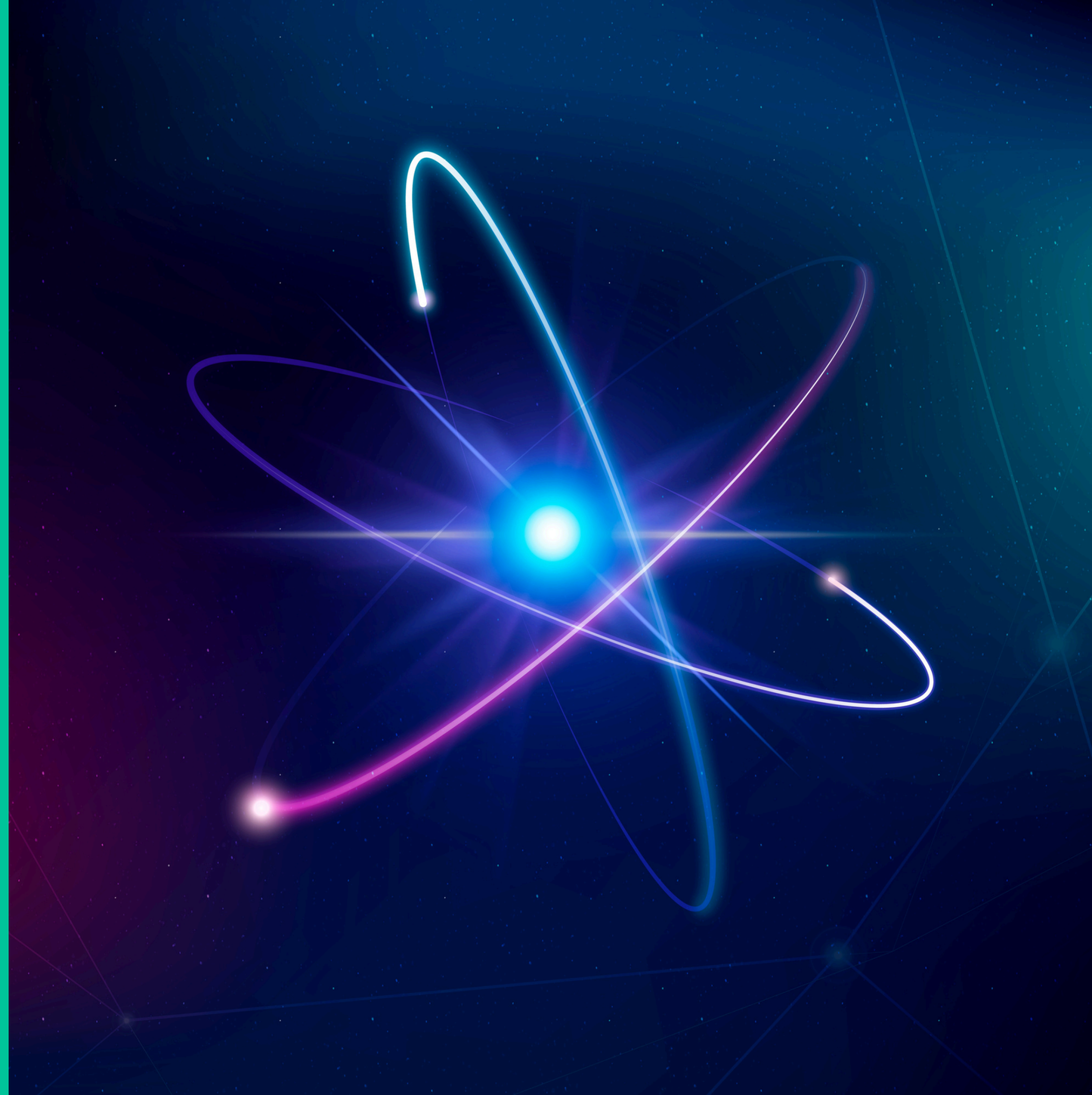


Fig.: Representation of photon polarization for B92 protocol

$$|\langle A|H\rangle|^2 = \frac{1}{2}, \qquad |\langle V|H\rangle|^2 = 0,$$
$$|\langle A|D\rangle|^2 = 0, \qquad |\langle V|D\rangle|^2 = \frac{1}{2}.$$

1a	1	0	1	1	0	0	0	1	0	0	1	1	0	1	0	1	0	1	1	0	0	1	0	1
1b	H	D	H	H	D	D	D	H	D	D	H	H	D	H	D	H	D	H	H	D	D	H	D	H
2a	1	1	0	1	0	0	1	1	1	0	1	0	0	1	1	0	1	1	0	0	1	1	0	0
2b	A	A	V	A	V	V	A	A	A	V	A	V	V	A	A	V	A	A	V	V	A	A	V	V
3a	yes	no	no	yes	yes	yes	no	yes	no	yes	yes	no	yes	yes	no	no	no	yes	no	yes	no	yes	yes	no
3b	yes	-	-	-	yes	-	-	yes	-	yes	-	-	yes	-	-	-	-	yes	-	-	-	yes	-	-
Bob calls Alice																								
4	1	-	-	-	0	-	-	1	-	0	-	-	0	-	-	-	-	1	-	-	-	1	-	-
5a	1	-	-	-	0	-	-	0	-	1	-	-	0	-	-	-	-	1	-	-	-	0	-	-
5b	yes	-	-	-	-	-	-	-	-	yes	-	-	-	-	-	-	-	yes	-	-	-	-	-	-
6	-	-	-	-	0	-	-	1	-	-	-	-	0	-	-	-	-	-	-	-	-	1	-	-

- Challenges



The B92 protocol still faces several challenges: -:

1. Polarization Decoherence: Polarization states can decohere during propagation, especially in optical fibers. Decoherence can lead to errors in bit detection and compromise the security of the key. Maintaining polarization purity over long distances is a significant challenge.
2. Detector Performance: The performance of the detectors at Bob's side plays a critical role in the success of the B92 protocol. High quantum efficiency (QE) and low dark count rates are essential to maximize the probability of correctly detecting the transmitted photons and minimize noise.
3. Synchronization: Precise synchronization between Alice and Bob's clocks is crucial for aligning the sending and receiving of bits. Synchronization errors can lead to misalignment and loss of data. Maintaining synchronization over long distances and in the presence of network latency is a challenge.
4. Security Verification: Verifying the security of the generated key is essential to ensure that it is not compromised by Eve. This may involve performing statistical tests on the key to detect any anomalies or patterns that could indicate eavesdropping.

Thank You