BB84 Implementation on Custom QKD Setup

Irina Bradu

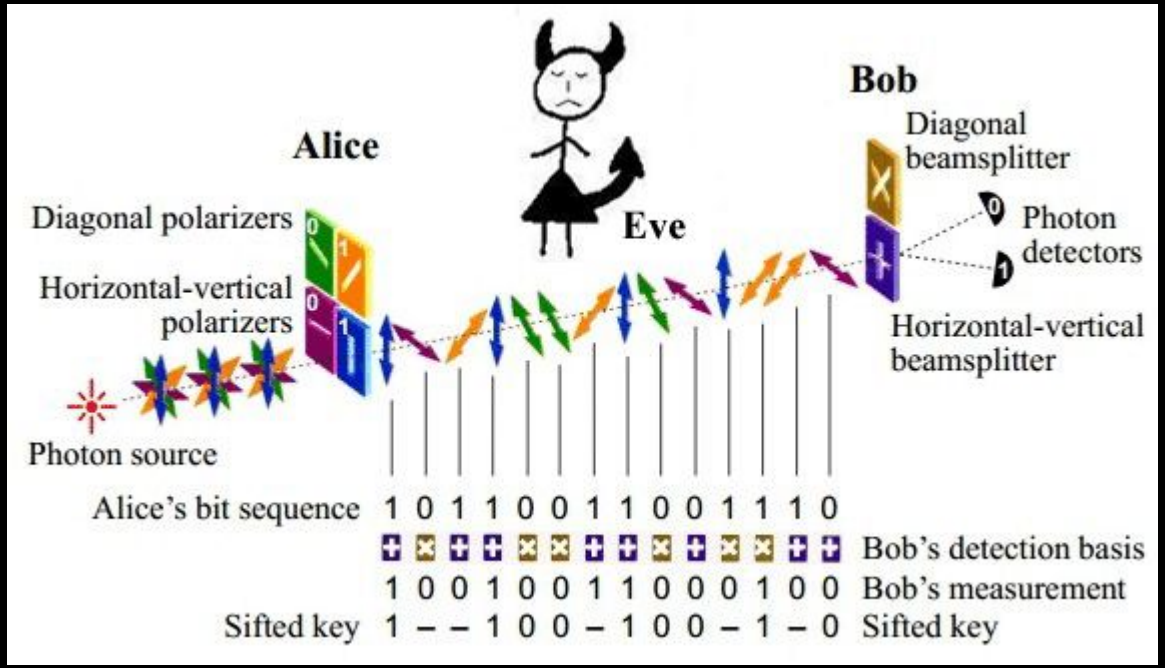
Thesis Advisors:

Prof. Dr. Pantelimon George Popescu
Dr. Ing. Alin-Bogdan Popa

Motivation

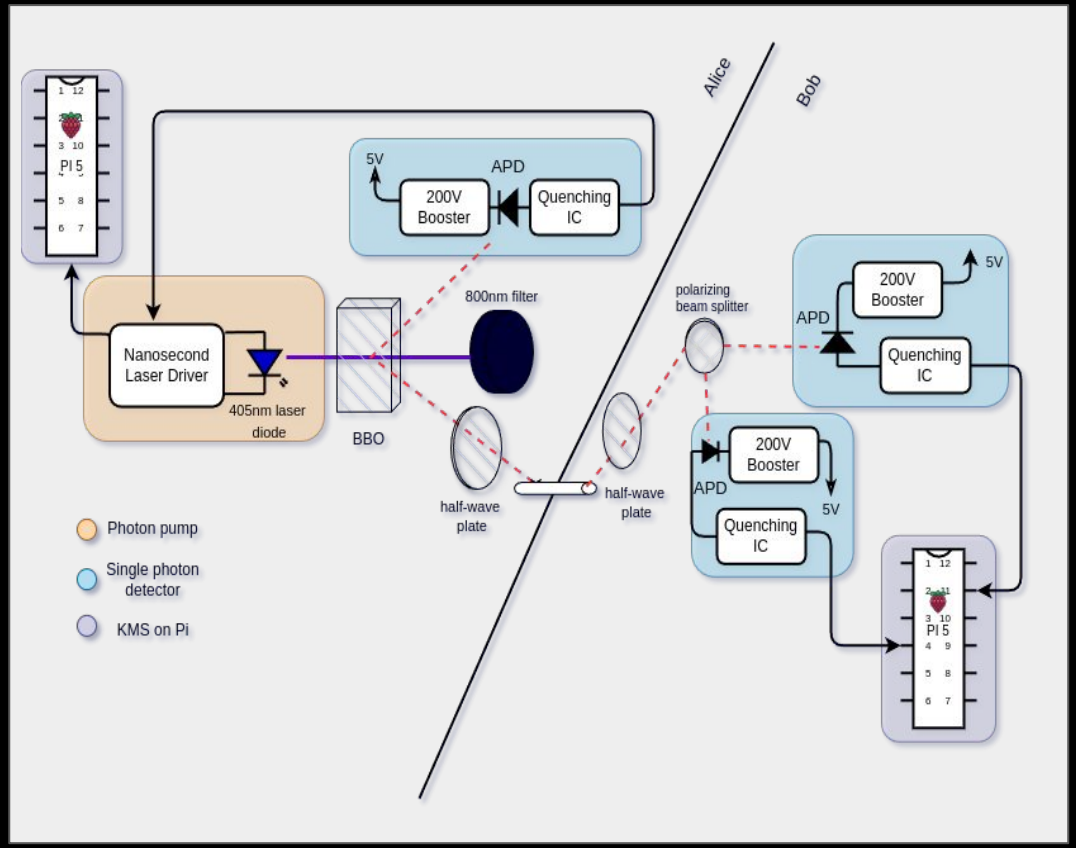
- Educational outreach 
- Hardware experimentation 
- Cost constraints 

BB84 recap



Credit : Weerasinghe, WAA Maheshya. "Quantum Cryptography." (2012).

Overview of the setup



Round	Alice Bit	Alice Basis	Bob Basis	Bob Result	Same Basis?
1	1	B	A	0	No
2	1	A	A	1	Yes
3	0	A	B	1	No
4	0	B	B	0	Yes
5	1	A	B	1	No
6	0	B	A	1	No
7	1	B	B	1	Yes
8	0	A	A	0	Yes

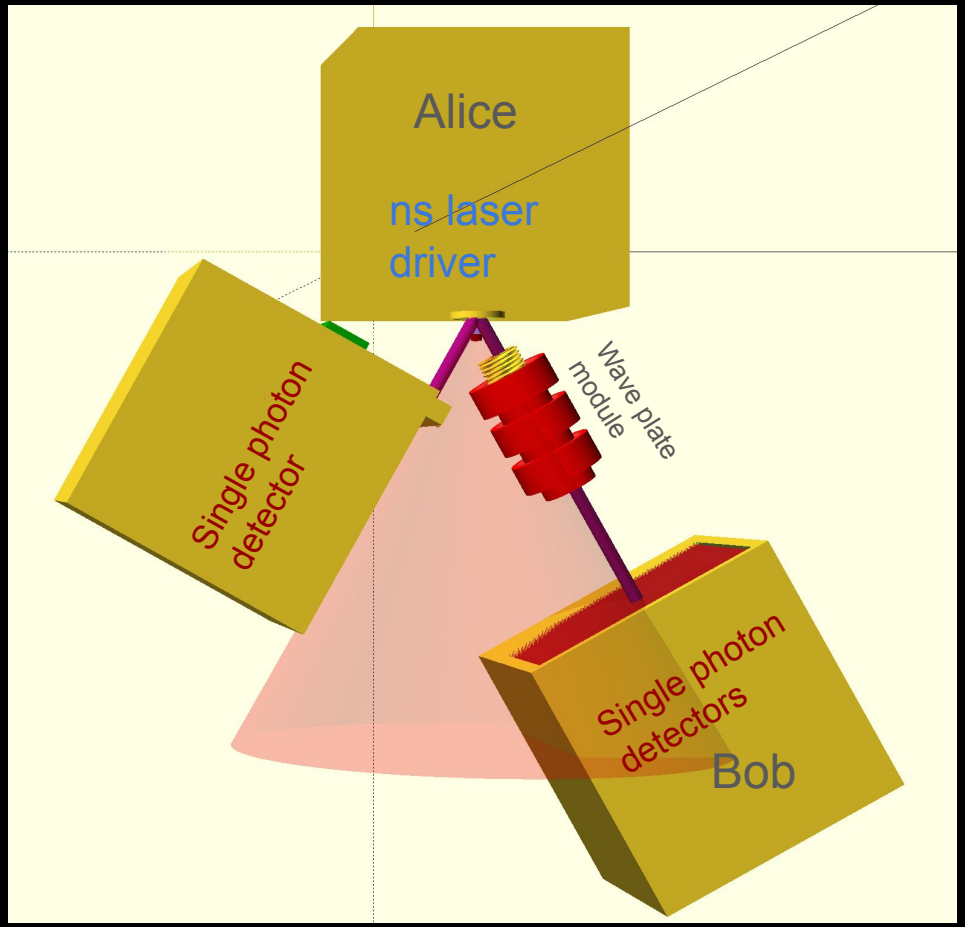
Target Base	Target State	Desired Polarization	HWP Angle (from H)
Z	H	0°	0°
Z	V	90°	45°
X	D	45°	22.5°
X	A	135°	67.5°

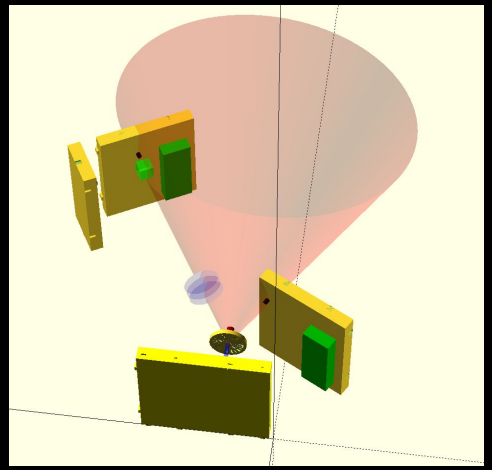
3D design

Modular design

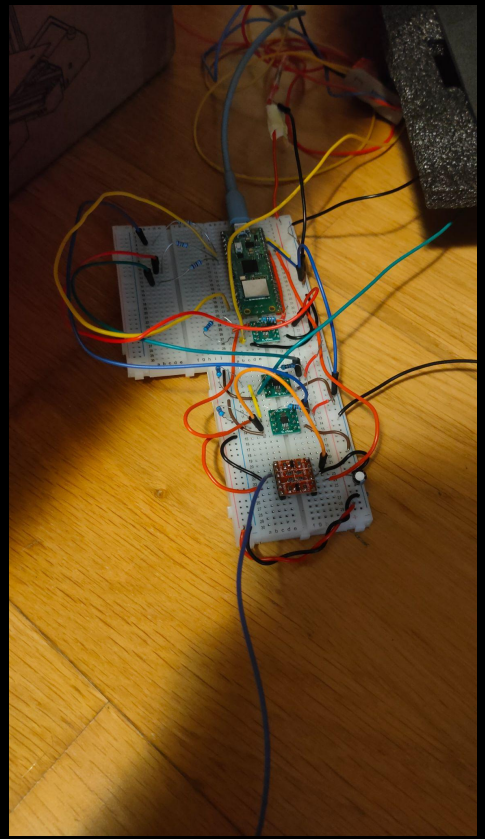
Compatible with

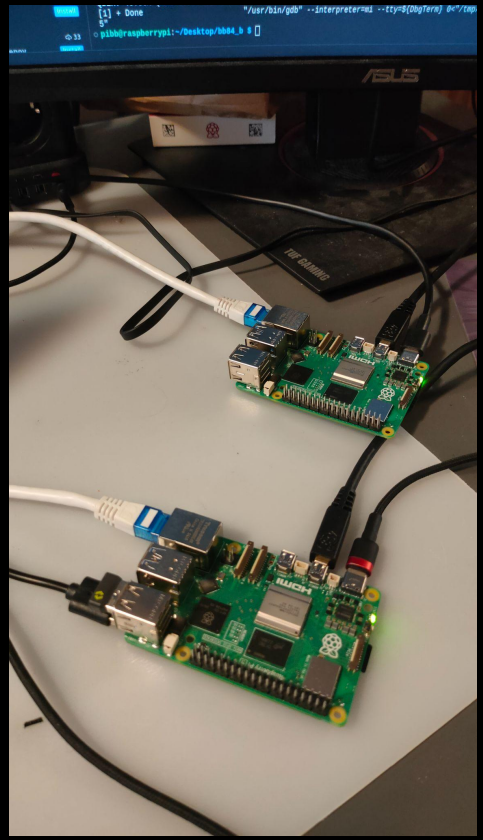
breadboards and PCBs





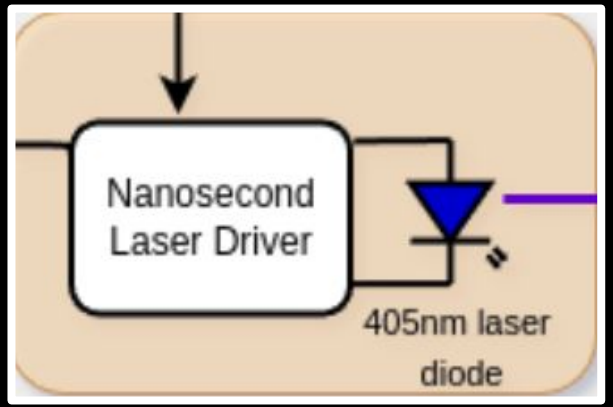
OpenScad



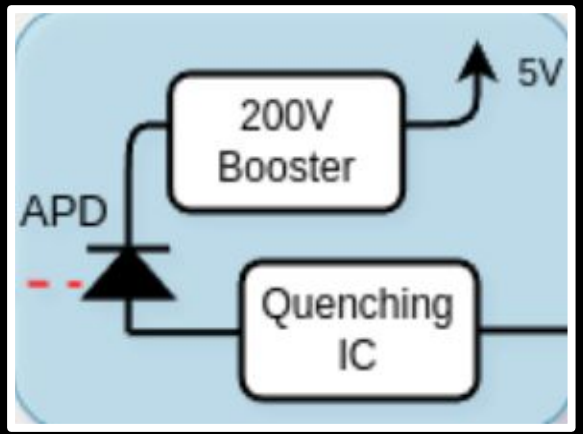

[1] + Done
"/usr/bin/gdb" --interpreter=mi --tty=${DbgTerm} 0<"/tmp
pibb@raspberrypi:~/Desktop/bb84_b $
ASUS
THE GAMING

Hardware Design

1

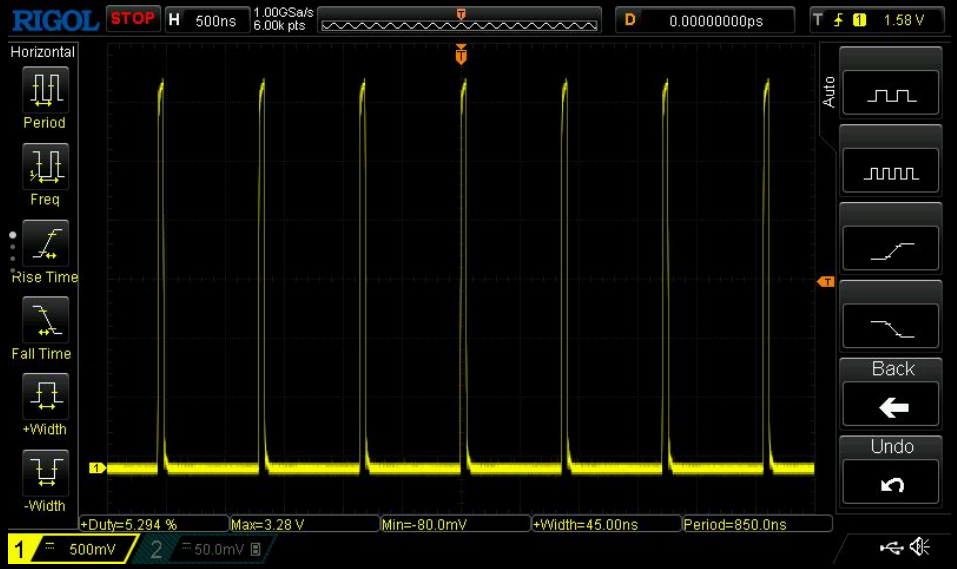


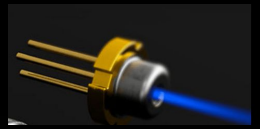
2

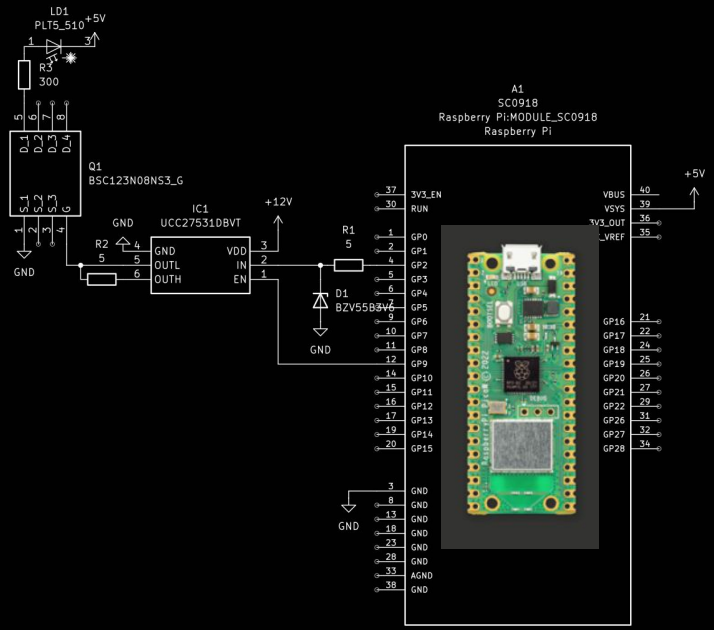


3

Hardware Design of the LASER driver



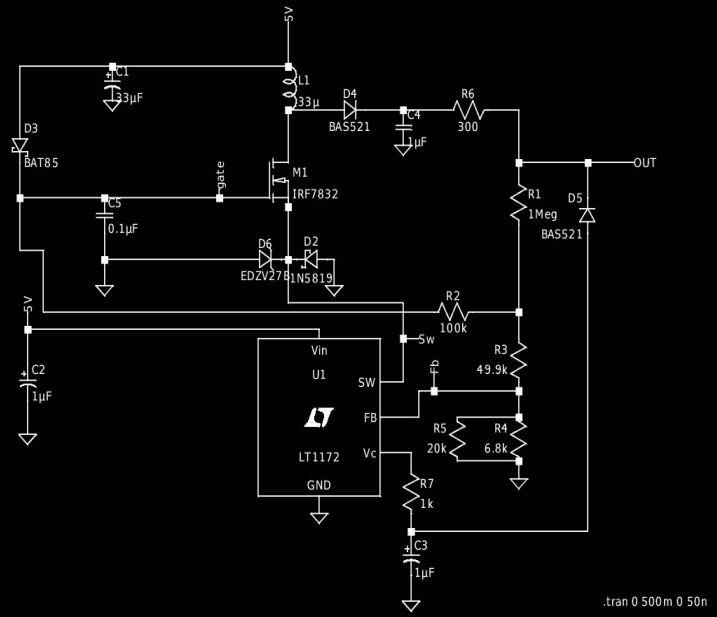




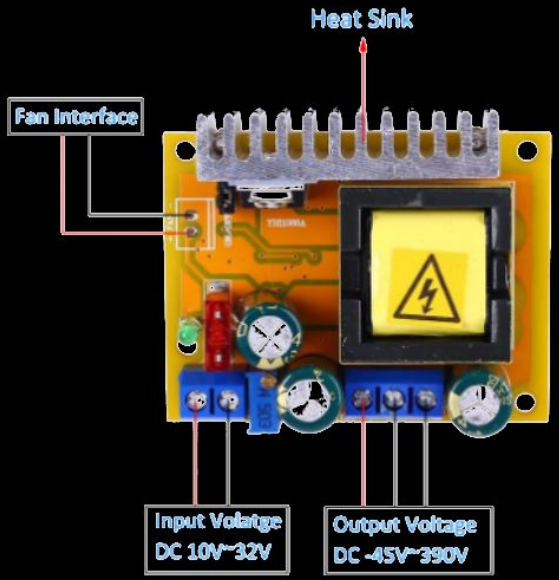
pio - 10ns per instruction

Hardware Design of the 5V to 200V Boost Converter

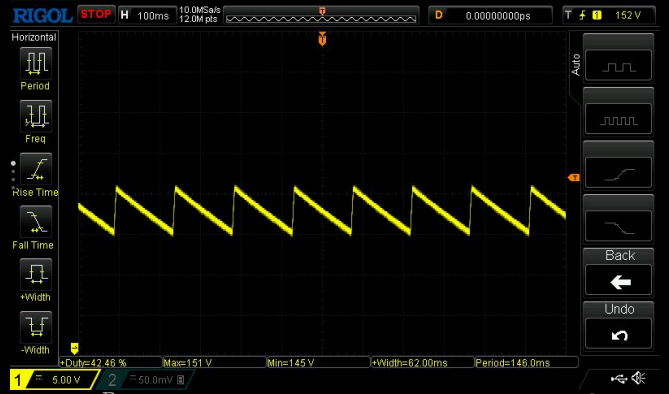
Jim Williams, AN98

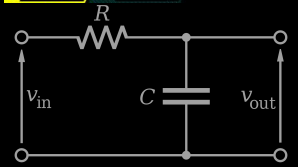


Hardware Design of the Adjustable Boost Converter



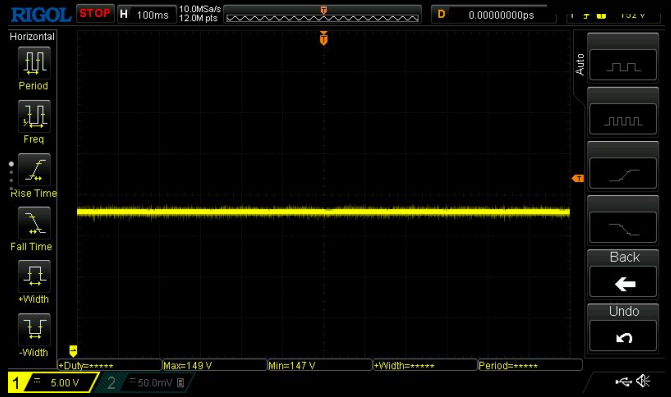
YH11068A



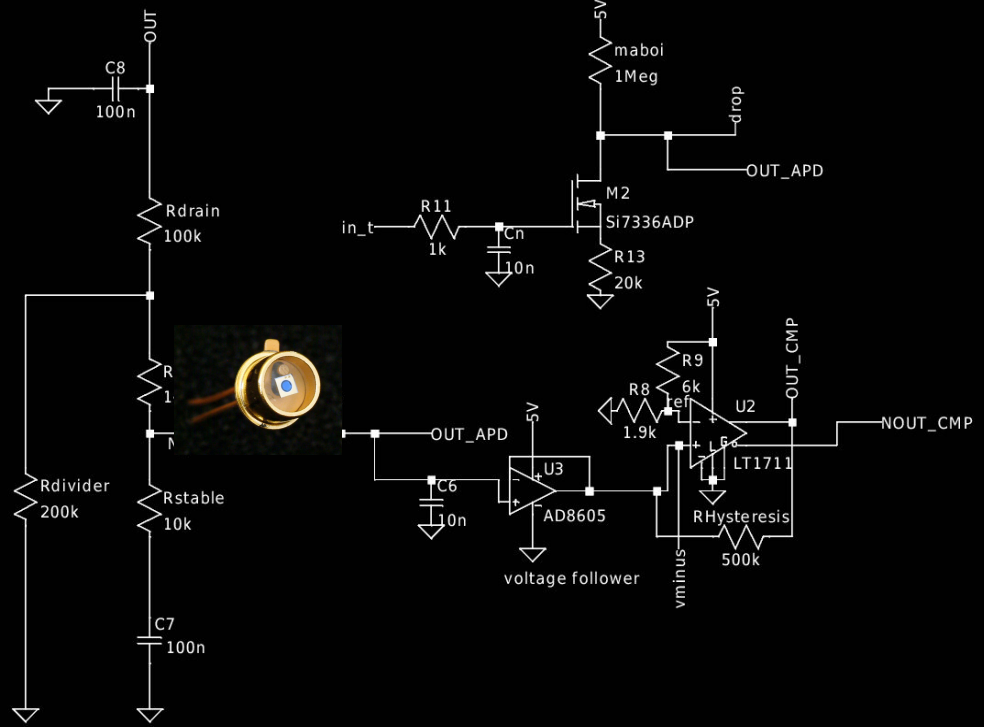


Low pass filter

Cut-off $\approx 0.16\,\mathrm{Hz}$

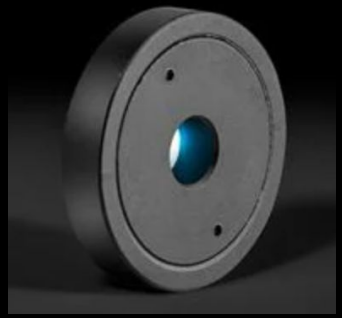


Hardware Design of the Single Photon Detector with Active Quenching



Optics and alignment considerations

Creating single photons



BBO crystal - Type 1 SPDC

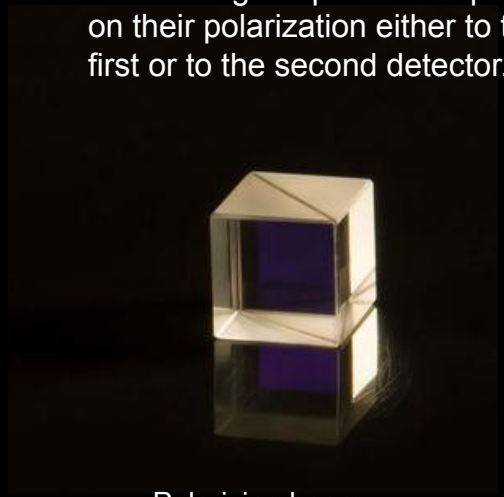
P/P@400-800 nm

Changing photon state and measurement basis

Half-wave plates

25mm Dia., λ/2 Retarder Film

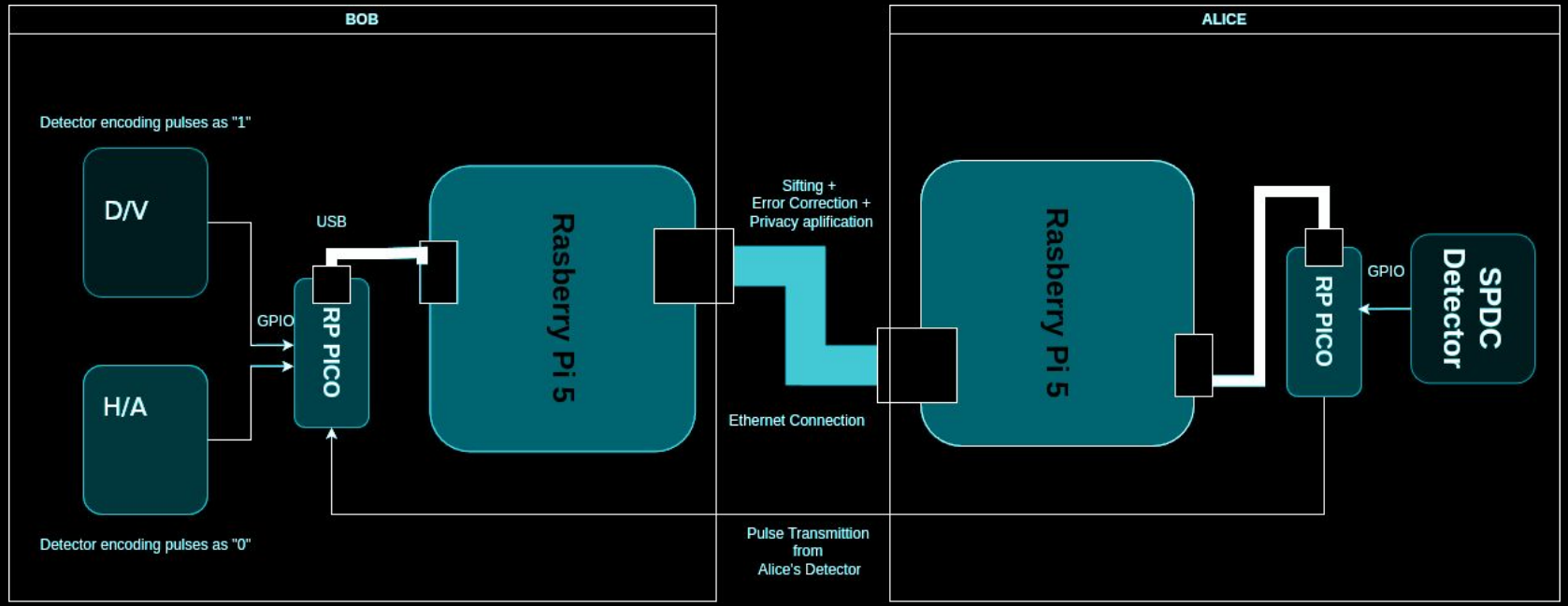
Redirecting the photons depending on their polarization either to the first or to the second detector.



Polarizing beam splitter

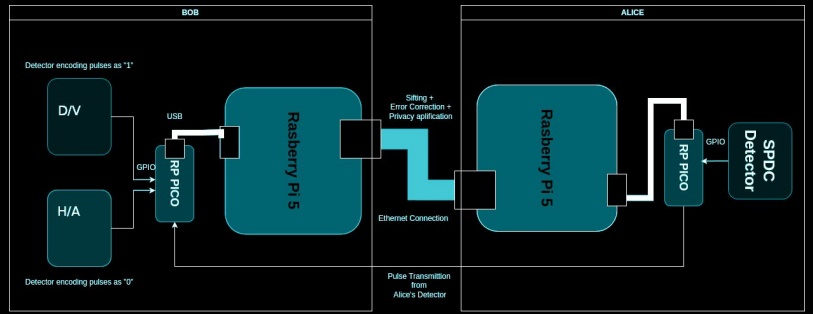
780nm Rs>99.5% Tp>95% 10 x 10 mm

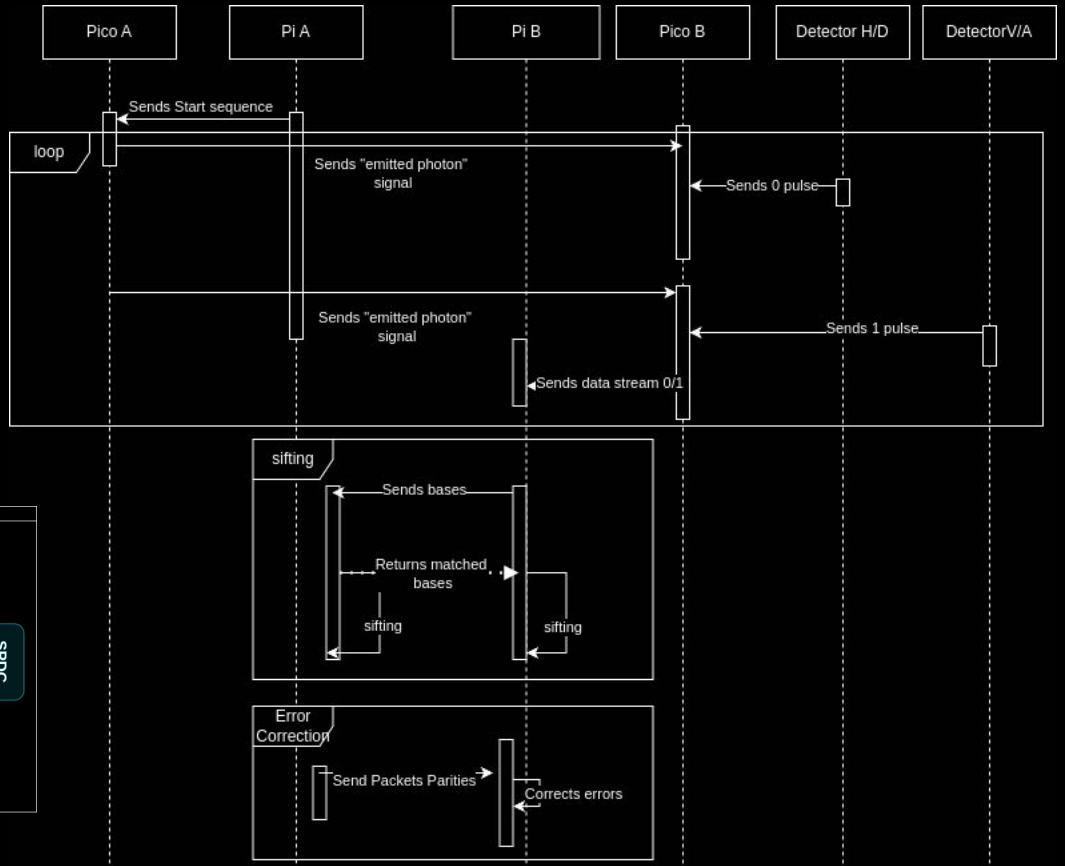
The software



The software

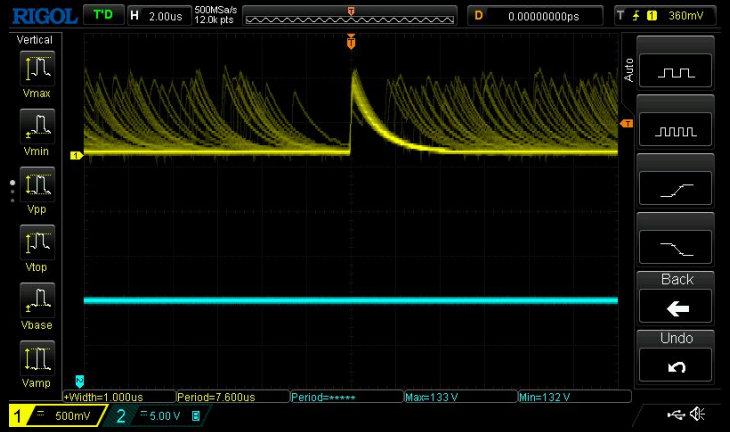
- Raw key storage
- Key Sifting
- Error Correction
- Calculating Qubit Error Rate





Results

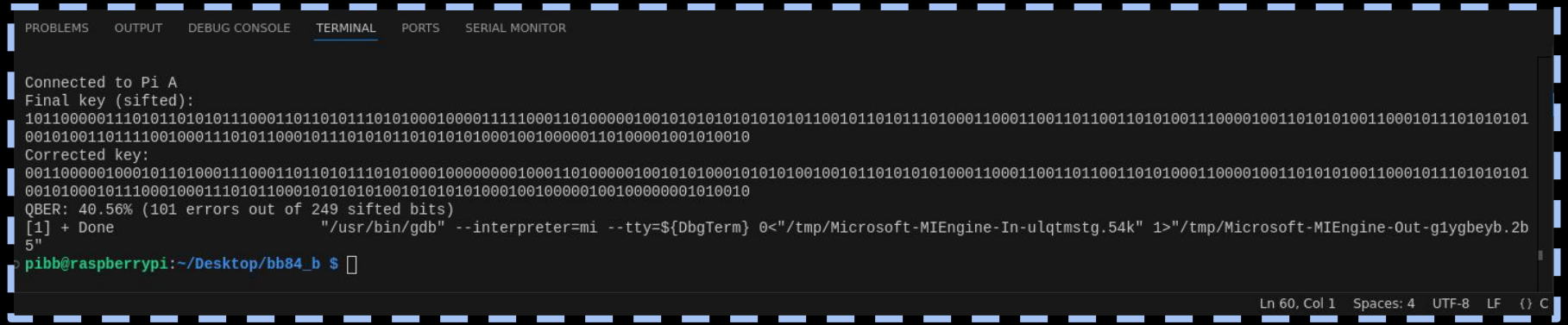
Pulses into clean 3V3 TTL signal



Results

average of 40% qubit error rate

$$\text{QBER} = \frac{\text{Number of mismatched bits}}{\text{Total number of sifted bits}}$$



Not usable unless we use super aggressive error correction which is not safe!

BB84 Implementation on custom QKD setup - Irina Bradu - June 2025

Future work

- Noise reduction -> Cooling
- Better single photon generation -> Refining optical alignment
- Higher photon detection rate -> Use SiPM (silicon photomultiplier)

https://github.com/irina-b-dev/custom-qkd-source