universidade
de aveiro

Ali, S., Saharudin, S. & Wahiddin, M. R. (2009). Quantum Key Distribution Using Decoy State Protocol. American Journal of Engineering and Applied Sciences, 2(4), 694-698.

Quantum Security Course - *Paper Presentation*

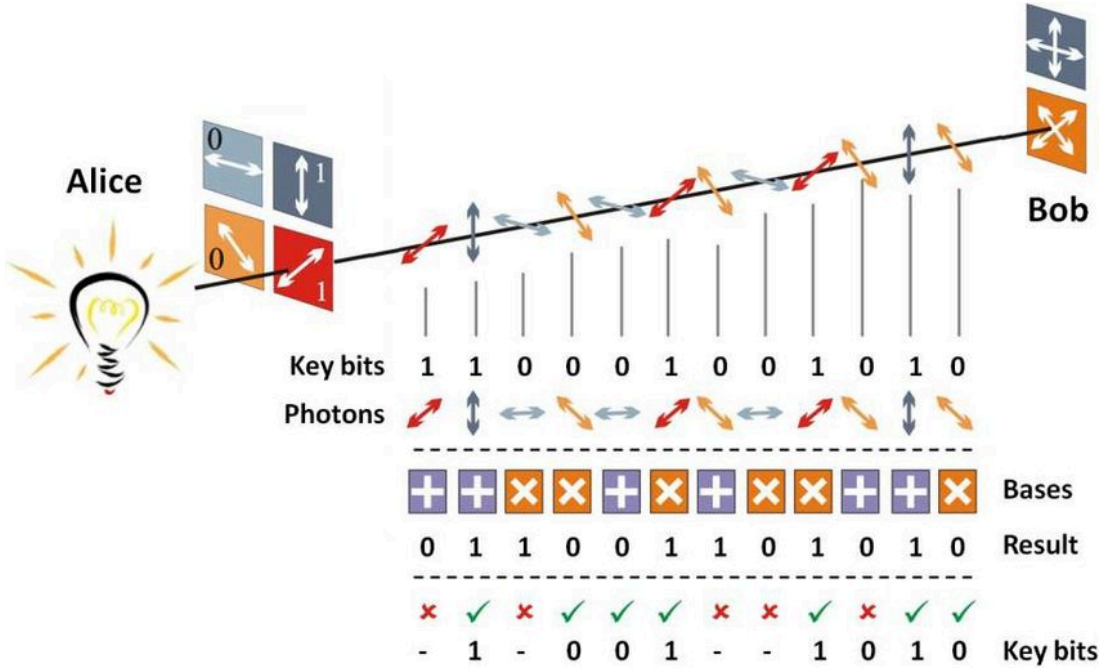
David Araújo (93444)

25th of October 2024

Context and Background

Quantum Key Distribution (QKD) can help two remote parties to set up the secure key by **non-cloning theorem**.

In theory, this ensures that these **states cannot be perfectly copied**, providing a layer of security against eavesdroppers.



Threats and Limitations

In a Photon-Number Splitting (PNS) attack, an eavesdropper (Eve) targets multi-photon pulses.

These can be split without disturbing the transmission, allowing Eve to intercept and retain one or more photons while letting the rest pass to Bob undetected.

Motivation for Decoy States

Using decoy pulses that are **intentionally designed to have an intensity similar to single-photon states** but with slight variability.

The decoy states help detect and mitigate PNS attacks by **analyzing discrepancies in photon detection rates**, while the GLLP security proof **ensures that the overall system remains robust** against potential vulnerabilities in realistic settings.

Key Generation Rate in QKD

Combining **signal states**, carrying most of the secret bits, with **weak and Vacuum states**, to detect eavesdropping, the improved QKD's key generation rate with high security is given by this formula.

Because BB84 is used, the subscript is:

$$q = \frac{1}{2}\frac{N_2}{N}$$

$$R \geq q\{Q_\mu f(E_{mu}) H_2(E_{mu}) + Q_1[1 - H_2(e_1)]\}$$

q	=	Depends on the protocol, the subscript
μ	=	The average photon number per signal in signal states
Q_μ	=	The gain of signal states
E_μ	=	The quantum bit error rate (QBER) of signal states
Q_1	=	The gain of the single photon states in signal states
e_1	=	The error rate of single photon states
f(x)	=	The bi-directional error correction rate[13]
H_2(x)	=	Binary shannon information function

$$H_2(x) = -xlog_2(x) - (1-x)log_2(1-x)$$

Real-life Implementation

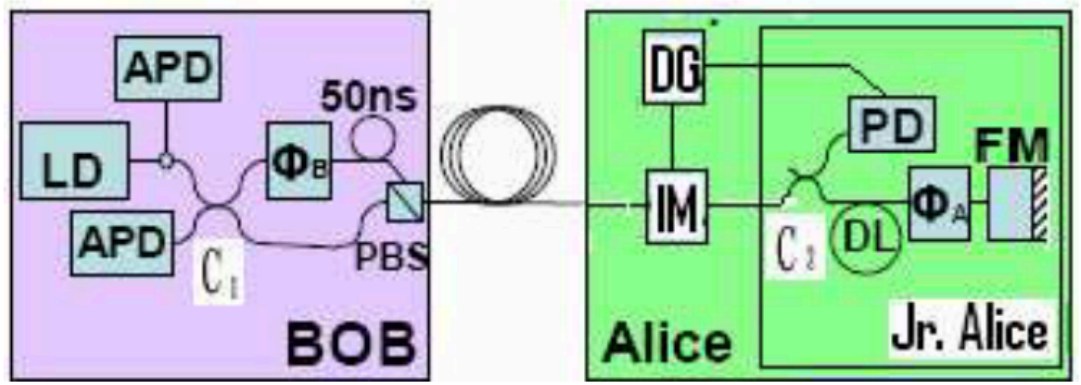
Bob will send frames of **624 NP pulses with a 200 ns intervals**, ensuring that the entire frame returns before the next is sent.

Using **phase-shift keying (PSK)** the information is encoded in the phase difference between two pulses sent along different paths with varying delays and phase shifts.

In our implementation, the attenuation is done by placing a VOA (variable optical attenuator) in Alice's side.

Detection Mechanism

1. **Decoy Intensity Modulator (IM)**: Allows all incoming pulses to pass through without attenuation by default
2. **Frame Synchronization**: The first of a frame of a pulses sent from Bob, triggers the Decoy Generator.
3. **Pulse Attenuation**: After a delay, the Decoy Generator dynamically attenuates each pulse. Some to the intensity of signal states, others to the intensity of decoy states.



Experimental Results

Intensities chosen for the signals and weak states:

μ = 0.55, v = 0.152

Numbers of pulses used as signal, weak decoy and vacuum states are:

$N_\mu = 0.645N;\ N_v = 0.203N;\ N_0 = 0.162N$

Total number of pulses sent:

N = 105Mbit

Both, the lower bound of the gain in signal states and upper bound of the error rate, in single photon states are given by:

$$Q_1 \geq Q_1^L = \frac{\mu^2 e^{-\mu}}{\mu v - v^2}\left(Q_{1\,e}^{Lv} - Q_\mu e^\mu \frac{v^2}{\mu^2} - Y_0^U \frac{\mu^2 - v^2}{e_0 \mu^2}\right)$$

$$e_1 \leq e_1^U = \frac{E_\mu Q_\mu - e_0 Y_o^L e^{-u}}{Q_1^L}$$

Comparative Analysis

The **gain** and **error rates** for a perfect single photon were calculated with a **10 standard deviations** for a conservative estimate.

Even so, a lower bound for the key generation rate per pulse is found, which means a final key length of about:

$$L = NR = 66kbit$$

Table 1: Direct results from our experiment

Para	Value	Para	Value	Para	Value
Q_μ	0.0094	E_μ	0.0107	q	0.319
Qv	0.0027	Ev	0.0221	f (E)[13]	1.22
				Y_0	6.2×10^{-5}

Table 2: The lower bounds of Q_1, R^L and the upper bound of e_1.The values are calculated from Eq. 1-4, taking statistical fluctuation into account

Para	Value	Para	Value
Q_1^L	0.0037		
e_1^U	0.0271	R^L	6.2931×10^{-4}

$$R^L = 6.2931 * 10^{-4} \approx \frac{R_{perfect}}{4}$$