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*

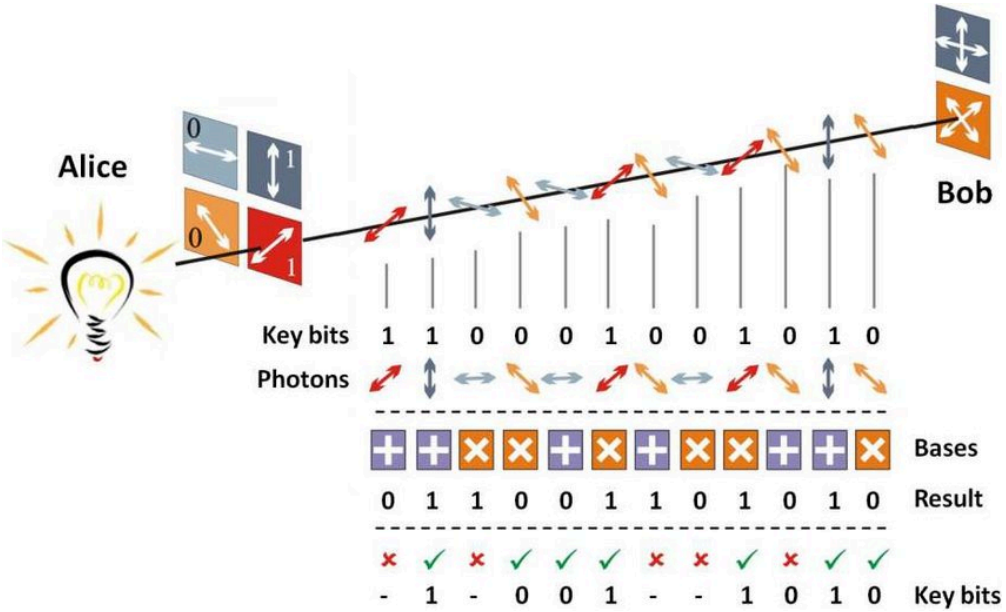
David Araújo (93444)

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

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

Signal states will carry most of the secret bits, while **weak and Vacuum states** are for detecting eavesdropping.

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

The improved QKD's key generation rate with high security is given by this formula:

$$R \geq q\{Q * \mu f(E * mu)H * 2(E * mu) + Q_1[1 - H_2(e_1)]\}$$

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

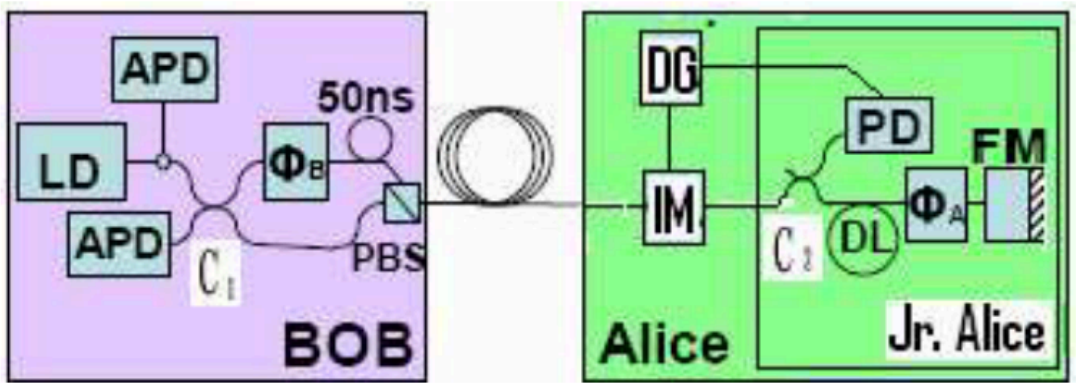
The **gain of the weak decoy state** and its **error rate** will result directly from experiments. Bounds for the **gain** and **error rate** of single photon states are given by:

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

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

Real-life Implementation

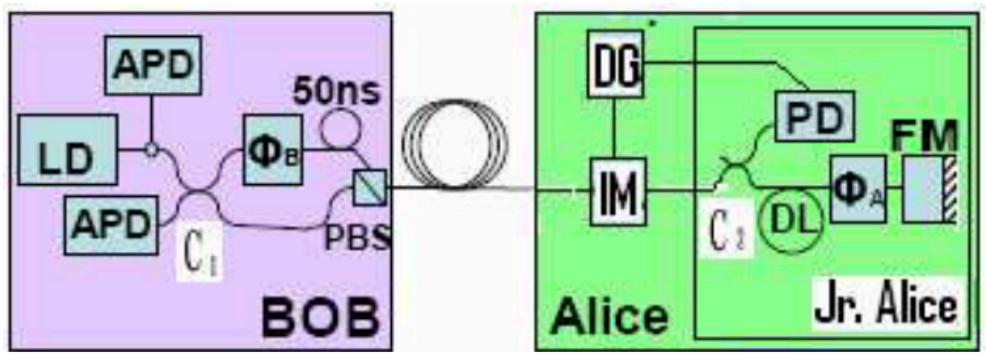
Bob will send frames of **624 NP pulses with a 200 ns intervals**, ensuring that the entire frame returns before the next is sent.



The **key is encoded** (using *PSK*) **in the phase between two pulses** traveling from Bob to Alice and back, emitted at Bob and separated at a first 50/50 Beam Splitter, having traveled through a shot and long arm, including a *Phase Modulator (PMb)* and a 50ns *Delay Line (DL)* respectively.

Decoy Modulation

1. **Decoy Intensity Modulator (IM)**: By default, all pulses pass through without attenuation. After the first pulse reaches coupler C2, a **synchronization signal will be output**.
2. **Frame Synchronization**: When the Decoy Generator is triggered, it will **hold for a delay time** before outputting a modulation voltage.
3. **Pulse Attenuation**: The Decoy IM will attenuate the intensity of each of the signals to that of the signal state of decoy state, dynamically.



Experimental Results

Intensities chosen for the signals and weak states:

$$\mu = 0.55;\ v = 0.152$$

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 by Alice:

$$N = 105Mbit$$

After the transmission of all *N* signals:

1. Alice broadcasts to Bob the distribution of decoy states.
2. Bob then announces which signal he received in correct basis
3. Both will calculate the gains and error rates of signal and decoy states.

Comparative Analysis

$$R^L = 6.2931 * 10^{-4}$$
$$L = NR$$

A final key length of *66 kbit* is found.

Even with a conservative estimation for a confidence within 10 standard deviations:

$$R^L \approx \frac{R_{perfect}}{4}$$

This hints that **small data sizes** and **few decoy states** are sufficient!

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}

Conclusion

For this set-up, at a distance of 25 km, without decoy states, it **wouldn't be possible to prove the security** of this protocol in an analogous manner.

With simple modifications to commercial QKD systems, decoy QKD allows **high key rate generation with unconditional security** against PNS attacks.

Questions ?