UNIVERSIDAD POLITECNICA DE VALENCIA
Instituto de Telecomunicaciones y Aplicaciones Multimedia
OQCG
Optical and Quantum Communications Group
OPTICAL AND QUANTUM COMMUNICATIONS GROUP
iTEAM Research Institute, Edificio 8G - Access D
C/ Camino de Vera s/n - 46022 – Valencia (Spain)
Tel. +34.96.387.95.80 - infogco@gco.upv.es

Cryptography and Quantum Key Distribution: A Telecom insight

Arturo Ortigosa-Blanch
José Capmany Francoy

aortigos@iteam.upv.es

1. **Introduction and overview**

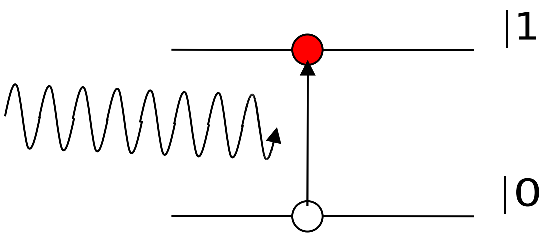
2. **QKD protocols: the BB84 protocol and others**

3. **Engineering aspects of QKD systems**

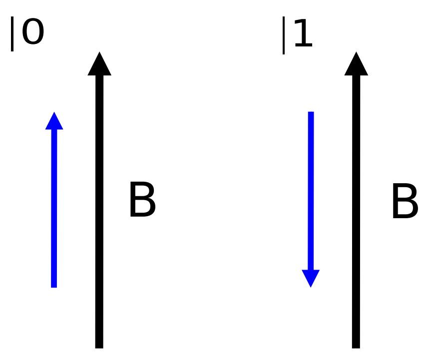
Quantum bits or qubits

A quantum bit (qubit) is a bit of information that can be represented through a 2 state quantum system

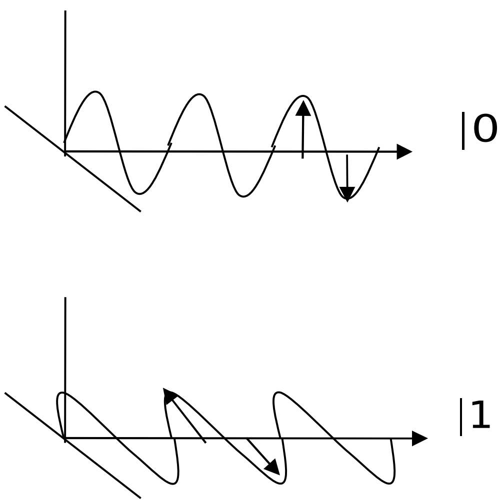
An electron of an atom



The spin in a magnetic field



A polarized photon



Quantum Cryptography: Public Key distribution and coin tossing

Bennett, C. H (IBM Research, Yorktown Heights)., and G. Brassard (University of Montreal), 1984, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing*, Bangalore, India, (IEEE, New York), pp.175–179.

When elementary quantum systems, such as polarized photons, are used to transmit digital information, the uncertainty principle gives rise to novel cryptographic phenomena unachieveable with traditional transmission media, e.g. a communications channel on which it is impossible in principle to eavesdrop without a high probability of disturbing the transmission in such a way as to be detected. Such a quantum channel can be used in conjunction with ordinary insecure classical channels to distribute random key information between two users with the assurance that it remains unknown to anyone else, even when the users share no secret information initially. We also present a protocol for coin-tossing by exchange of quantum messages, which is secure against traditional kinds of cheating, even by an opponent with unlimited computing power, but ironically can be subverted by use of a still subtler quantum phenomemon, the Einstein-Podolsky-Rosen paradox.

I. Introduction

Conventional cryptosystems such as ENIGMA, DES, or even RSA, are based on a mixture of guesswork and mathematics. Information theory shows that traditional secret-key cryptosystems cannot be totally secure unless the key, used once only, is at least as long as the cleartext. On the other hand, the theory of computational complexity is not yet

principle impossible to counterfeit, and multiplexing two or three messages in such a way that reading one destroys the others. More recently [BBBW], quantum coding has been used in conjunction with public key cryptographic techniques to yield several schemes for unforgeable subway tokens. Here we show that quantum coding by itself achieves one of the main advantages of public key cryptography by permitting secure distribution of random key information between parties who share no secret information initially, provided the parties have access, besides the quantum channel, to an ordinary channel susceptible to passive but not active eavesdropping. Even in the presence of active eavesdropping, the two parties can still distribute key securely if they share some secret information initially, provided the eavesdropping is not so active as to suppress communications completely. We also present a protocol for coin tossing by exchange of quantum messages. Except where otherwise noted the protocols are provably secure even against an opponent with superior technology and unlimited computing power, barring fundamental violations of accepted physical laws.

Offsetting these advantages is the practical disadvantage that quantum transmissions are necessarily very weak and cannot be amplified in transit. Moreover, quantum cryptography does not provide digital signatures, or applications such as certified mail or the ability to settle disputes before a judge.

1. INTRODUCTION: Quantum Cryptography

First commercial QKD system (2001)

…..Quantum cryptography could well be the first application of quantum mechanics at the single-quantum level..N. Gisin et al, Rev Mod. Phys (2002)

QKD: Key distribution under demand by means of quantum communications

- The detection and defeat of an eavesdropper is guaranteed by the laws of physics and the information theory
- It remains secure under the “quantum computer” and to any “tomorrow's technology”
- There is no possibility for passive eavesdropping
- It is compatible with existing telecommunication infrastructures

1. INTRODUCTION: Quantum Cryptography

Security is based upon the "One time pad" G.S. Vernam, Trans AIEE 45, 295 (1926)

- The key is a random sequence of bits with a length equal to the text to cipher
- XOR operation to cipher the message
- This is unconditionally secure if the key is used just once

ALICE

Text: 10000010
Key: 00110110

Cipher: 10110100

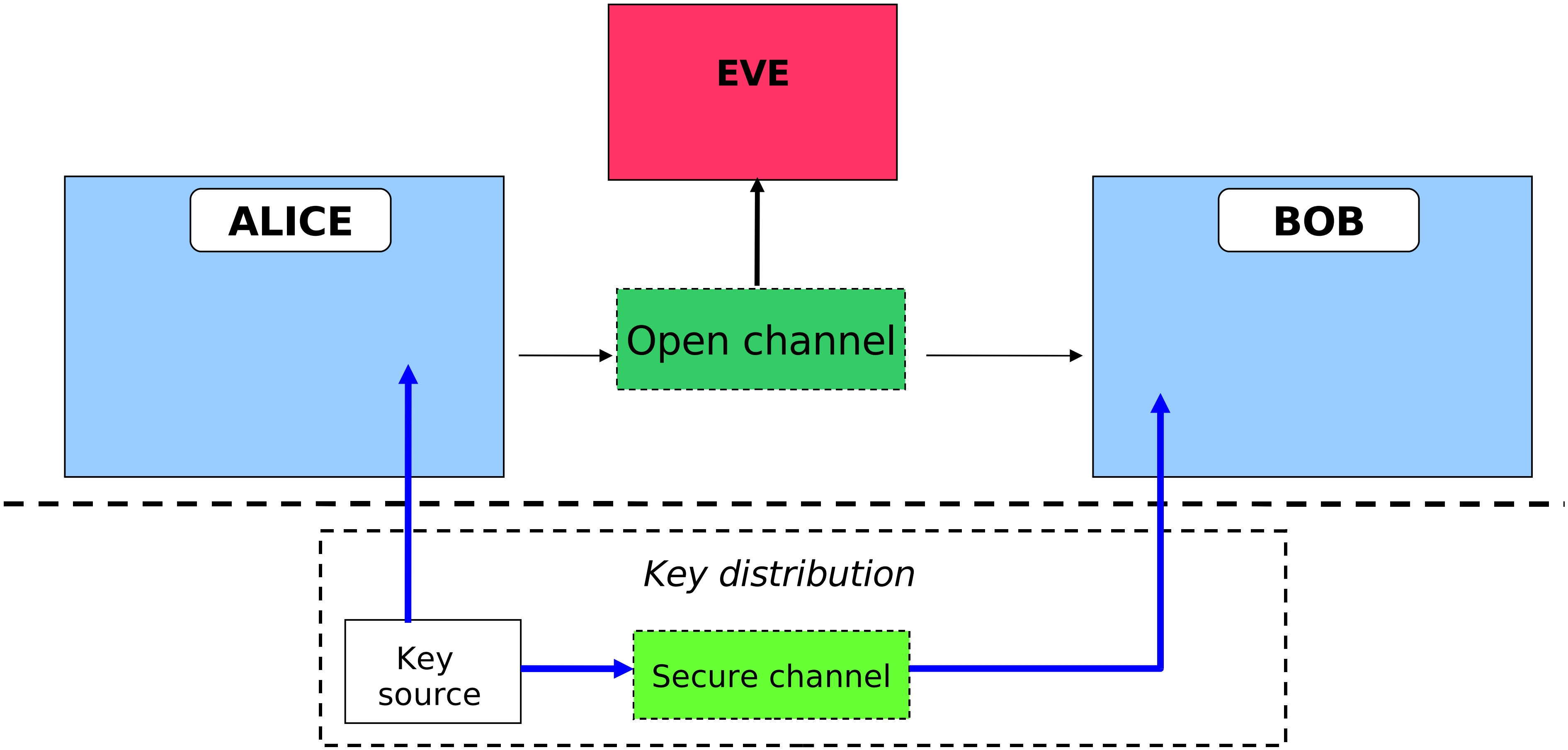
Public Channel

BOB

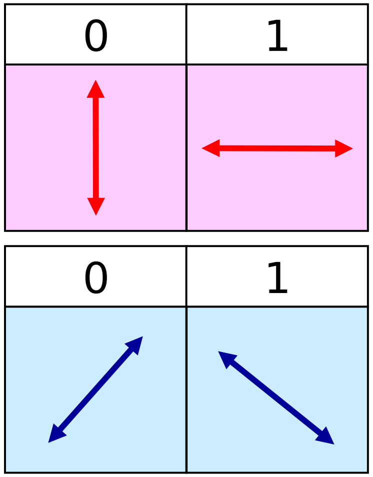
Cipher: 10110100
Key: 00110110

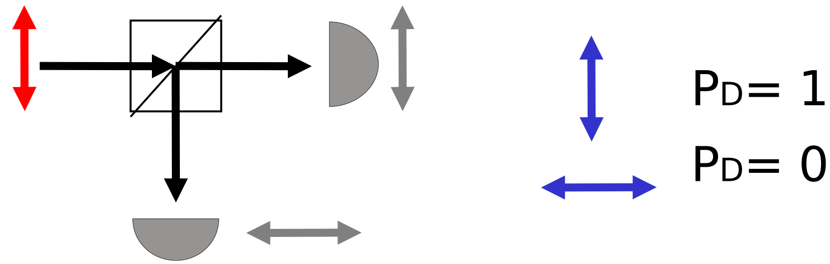
Text: 10000010

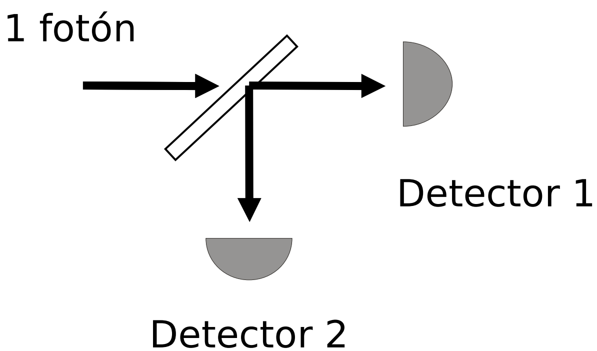
Quantum Key Distribution (QKD)

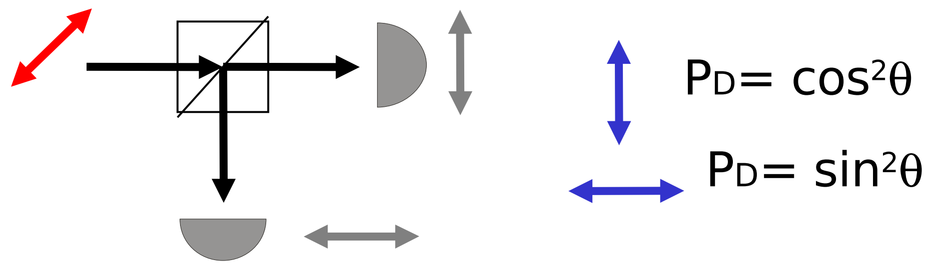


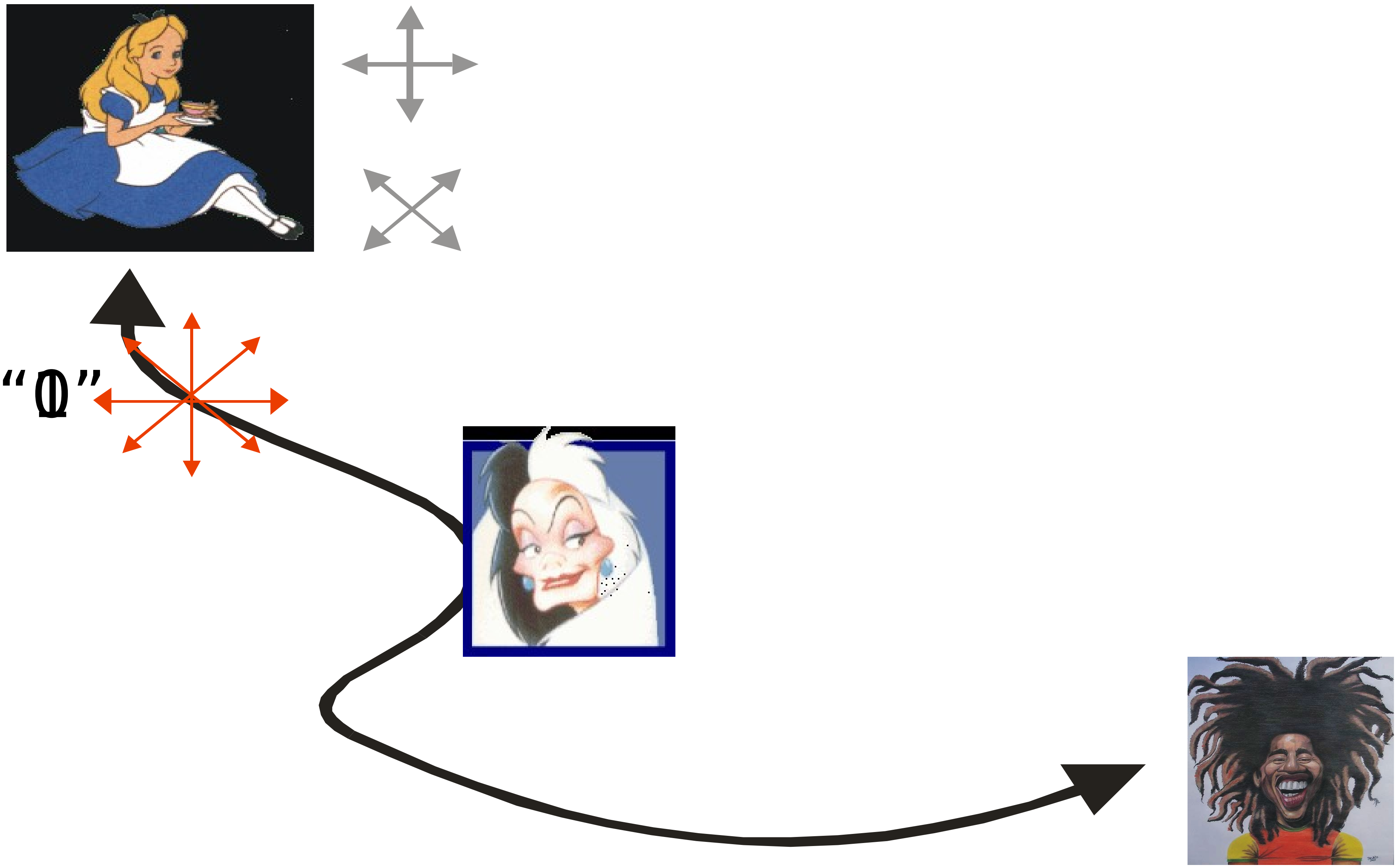
2. BB84 Protocol

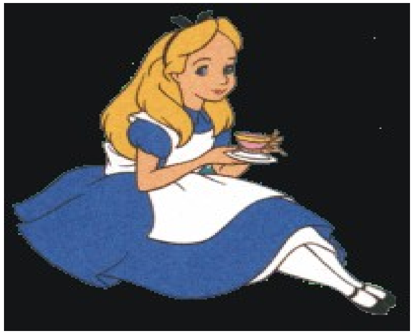




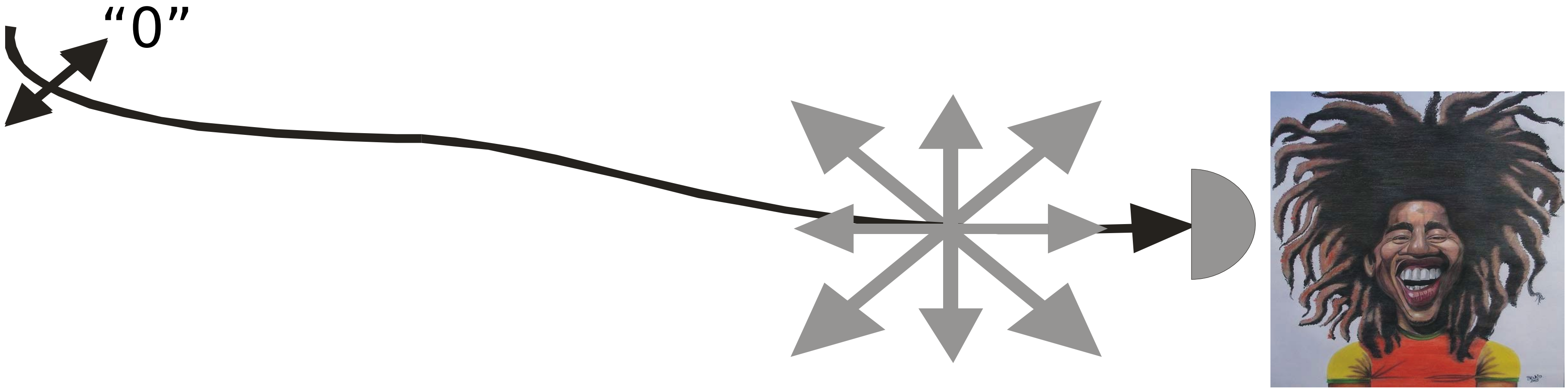


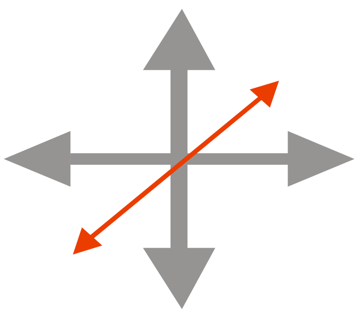



“0”

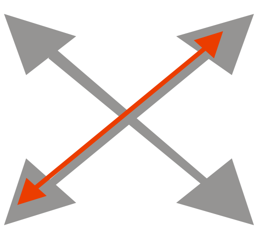


0	1	1	0	1	1	0	0	1	0
D	R	D	R	R	R	R	R	D	D
⤢	↕	⤡	↔	↕	↕	↔	↔	⤡	⤢



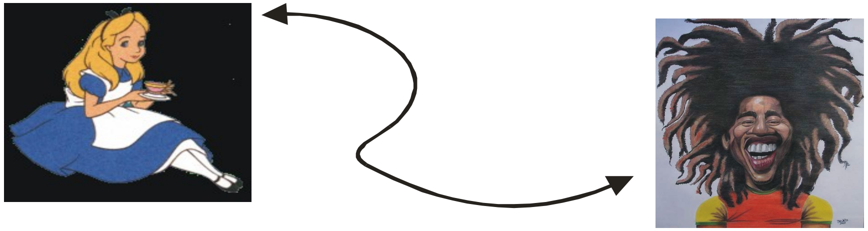


$P_D=1/2$



$P_D=1$

2. BB84 Protocol



0	1	1	0	1	1	0	0	1	0	1
D	R	D	R	R	R	R	R	D	D	R
⤢	↕	⤡	↔	↕	↕	↔	↔	⤡	⤢	↕
R	D	D	R	R	D	D	R	D	R	D
1		1		1	0	0	0		1	1

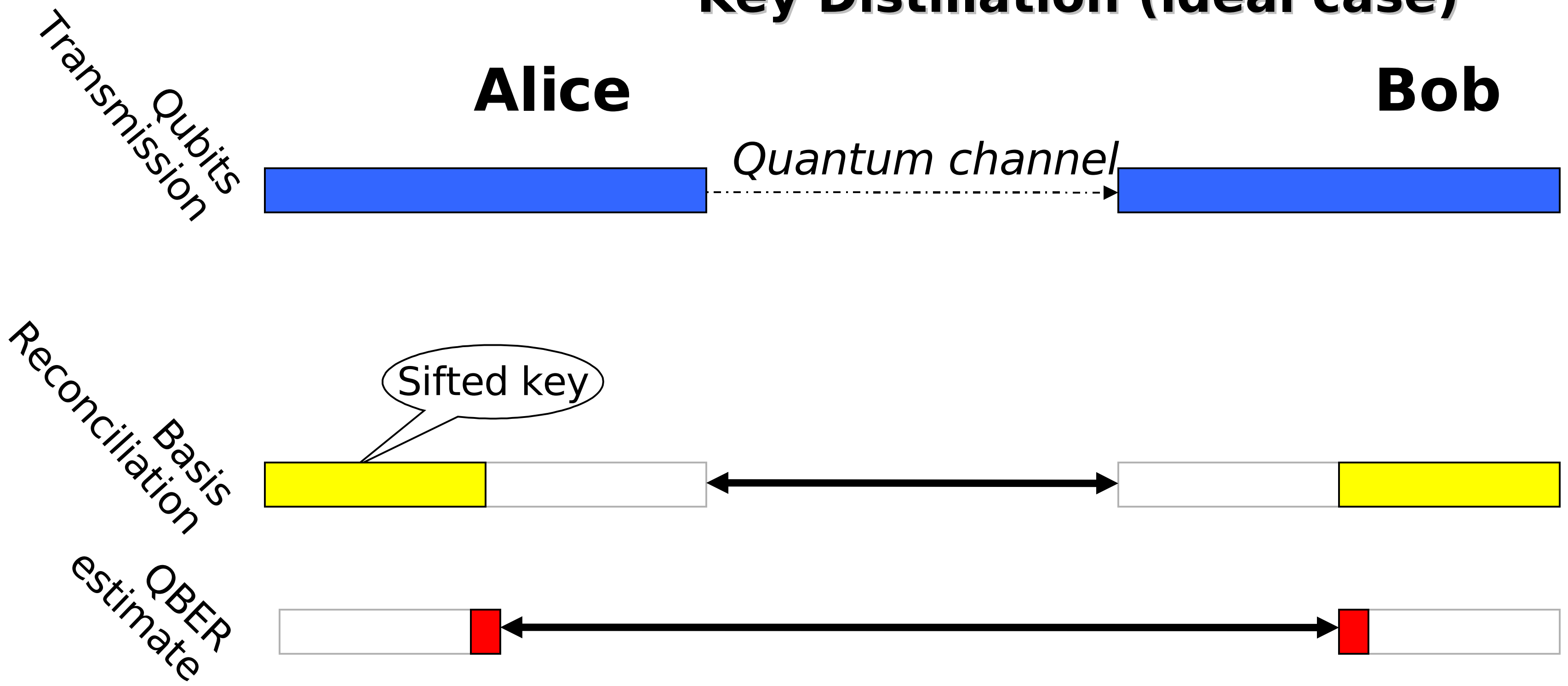
wrong detection

lost photon

Public discussion

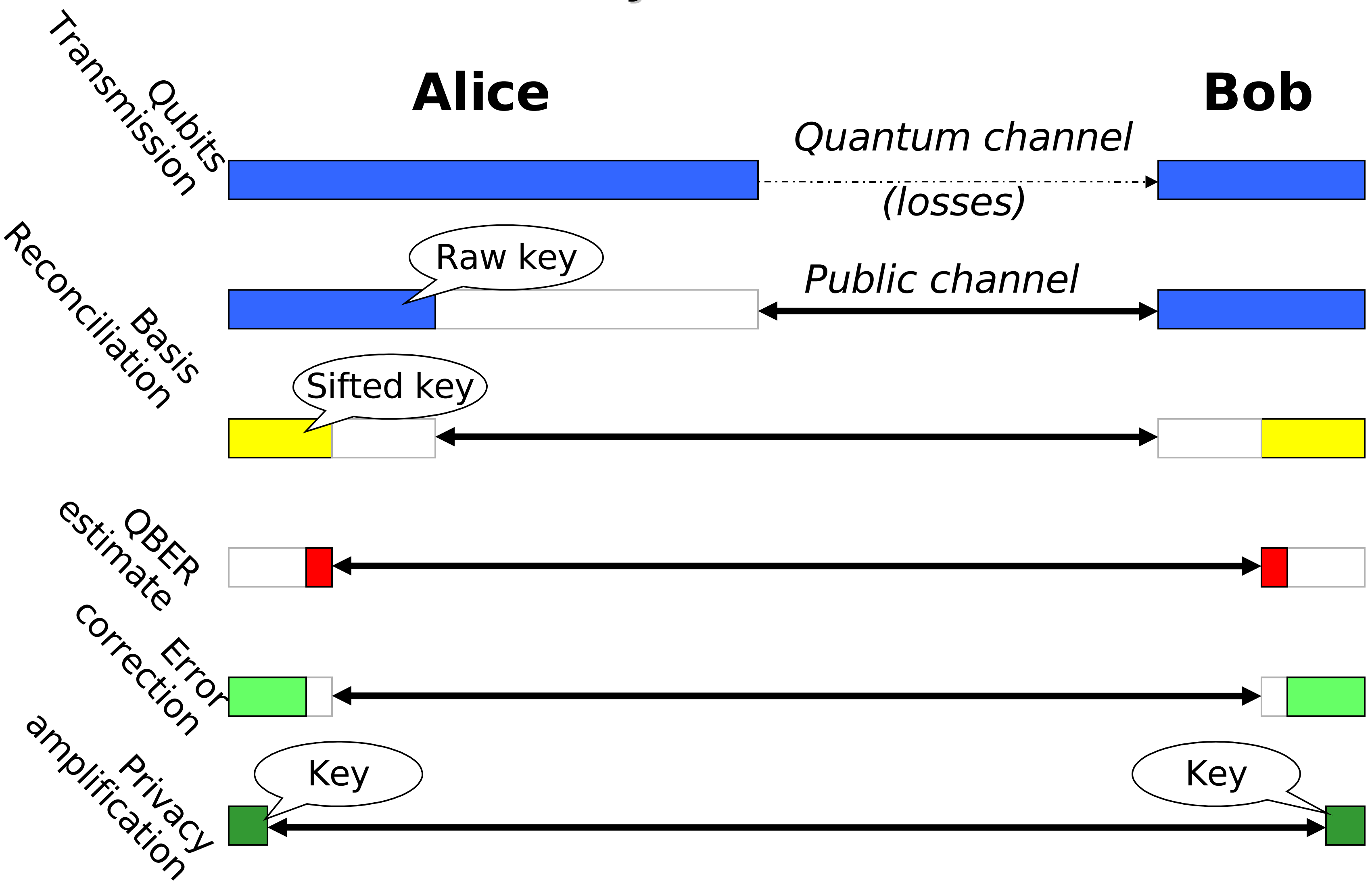
0	1	1	0	1	1	0	0	1	0
D	R	D	R	R	R	R	R	D	D
⤢	↕	⤡	↔	↕	↕	↔	↔	⤡	⤢
R	D	D	R	R	D	D	R	D	R
1		1		1	0	0	0		1
R		D		R	D	D	R		R
		OK		OK			OK		
		1		1			0		
				1					
		1					0		

Key Distillation (ideal case)



$$\text{QBER} = \begin{cases} 0 : \text{no eavesdropping} \\ > 0 : \text{eavesdropping} \end{cases}$$

Key Distillation (realistic case)



Some considerations about the communication between Alice y Bob:

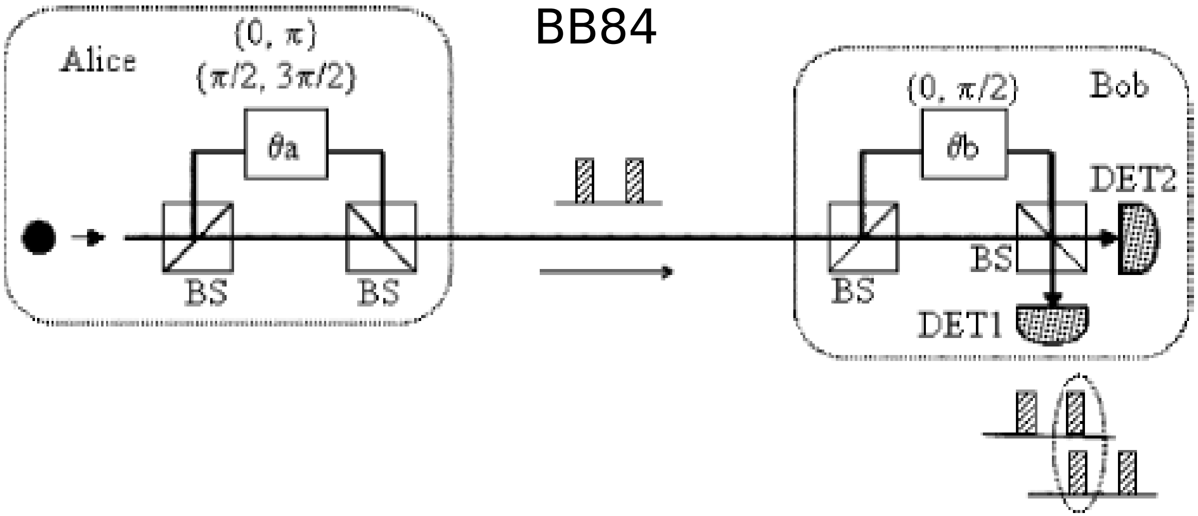
- The protocol is 50% efficient in the best case scenario
- Alice y Bob cannot predict how many, nor which, bits they will share
- Some photons are lost due to the channel losses
- Some photons lead to wrong detections because they come from outside the channel

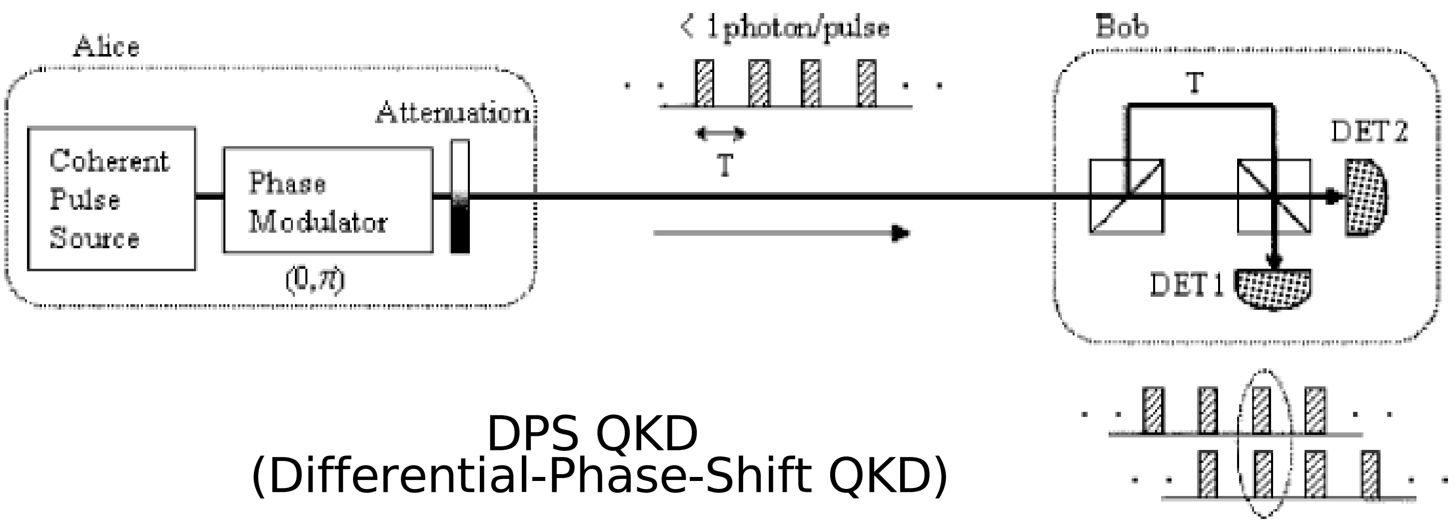
... nevertheless:

- Eve cannot passively monitor the channel (a photon cannot be split)
- Eve cannot copy any information
- This is key distribution and not info distribution
- You never discuss the key nor the info in the public channel

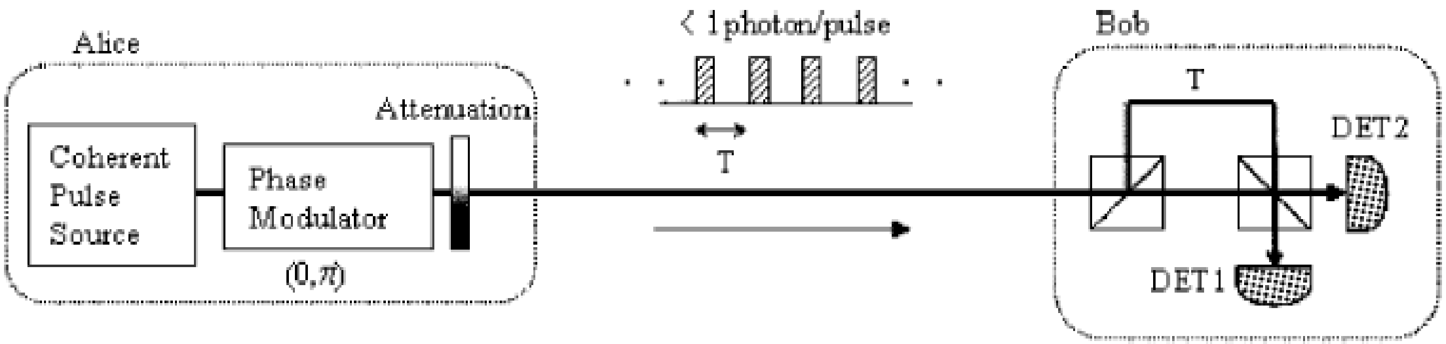
2. Other Protocols

BB84

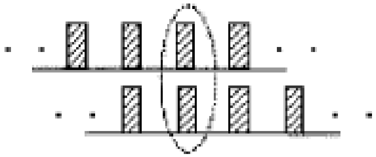




DPS QKD
(Differential-Phase-Shift QKD)



DPS QKD
(Differential-Phase-Shift QKD)



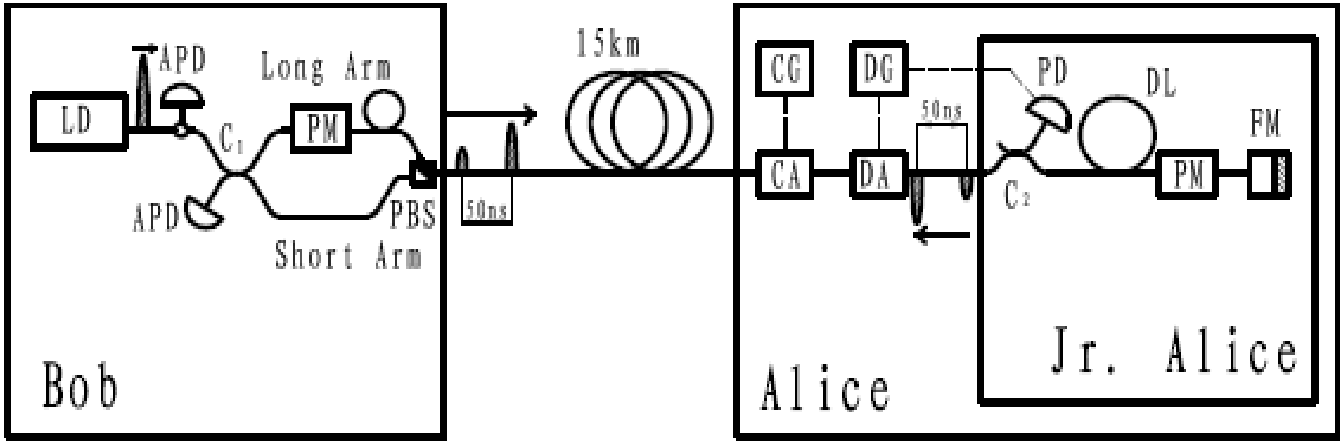
1) A pulse train is transmitted from Alice to Bob

2) After the transmission,Bob tells Alice the photon detection time

3) By referring to her modulation data, Alice knows which detector clicked at Bob's site

4) Alice and Bob create key bits by regarding the DET 1 click as bit "0" and the DET 2 click as bit "1."

only the detection time is disclosed, not the bit information



Decoy State Protocol

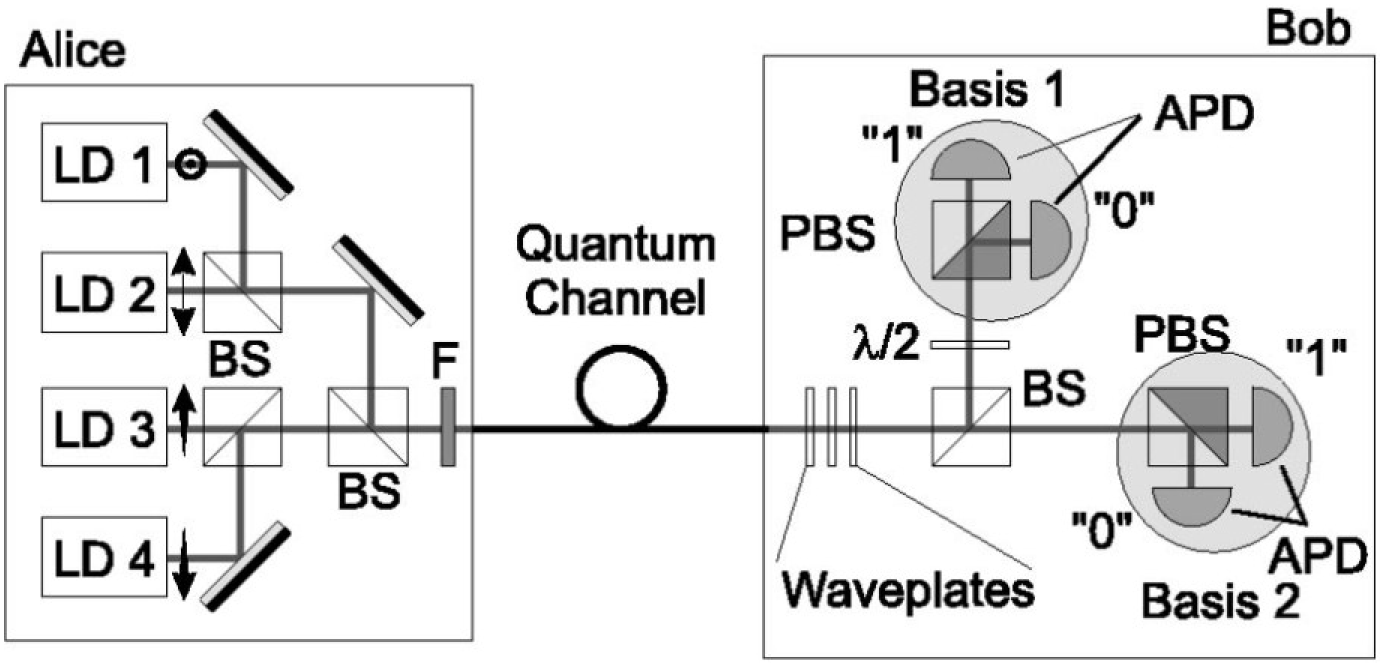
Alice introduces some some “decoy” states with average photon numbers besides the signal state

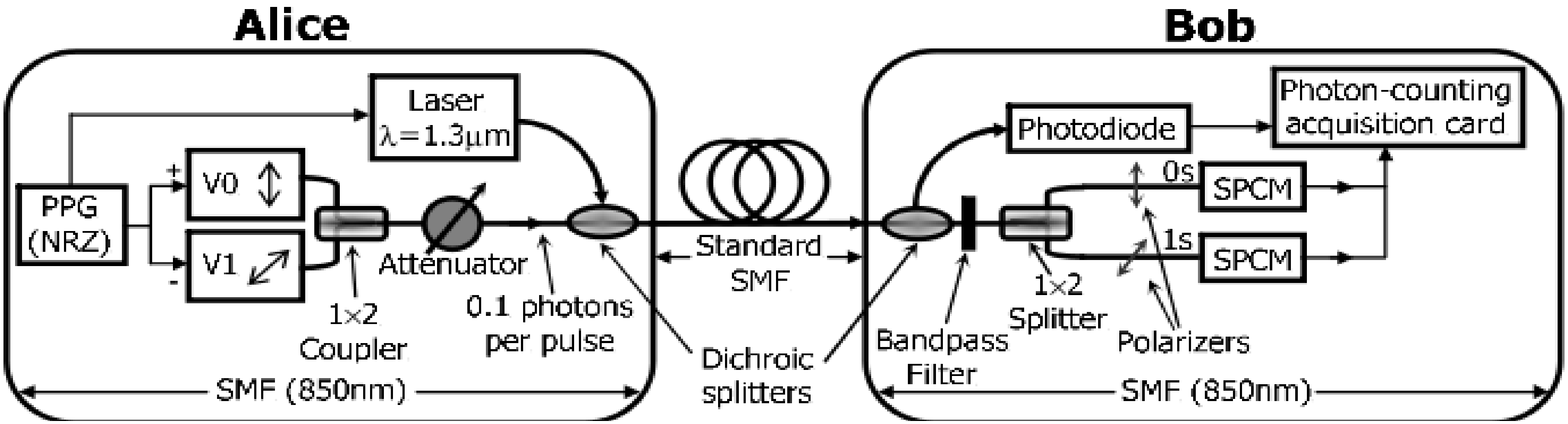
Alice announces the state of each pulse after Bob’s acknowledgement of receipt of signals. The statistical characteristics (i.e., gain and QBER) of each state can then be analyzed separately (the average photon number of certain state has only statistical meaning)

Eve’s attack will modify the statistical characteristics (gain or QBER) of decoy states and/or signal state and will be caught.

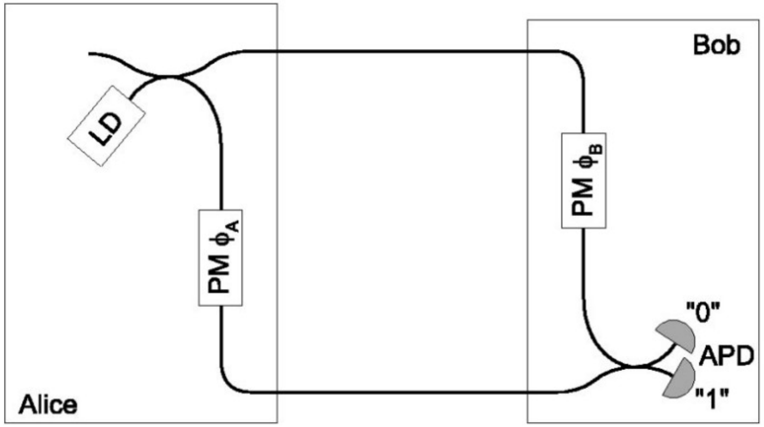
The decoy states are used only for catching an eavesdropper, but not for key generation

3. FIBER OPTIC SYSTEMS: Polarization Coding



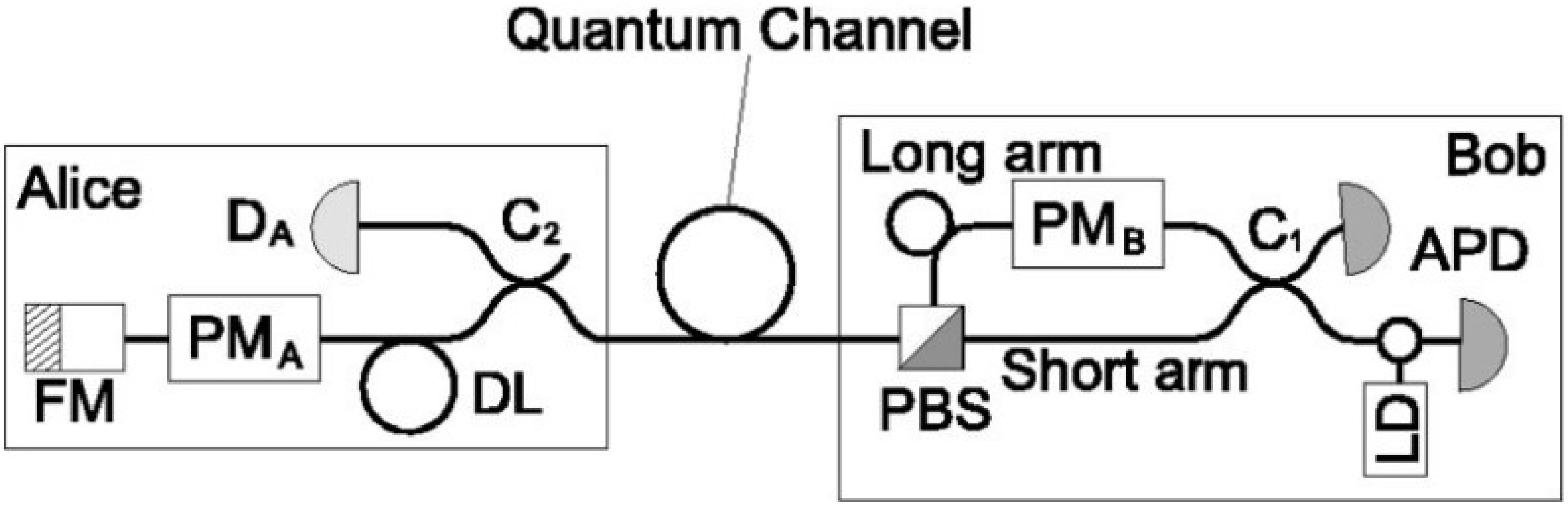


K. Gordon, V. Fernandez, G. Buller, I. Rech, S. Cova, and P. Townsend, "Quantum key distribution system clocked at 2 Ghz," Opt. Express 13, 3015-3020 (2005)

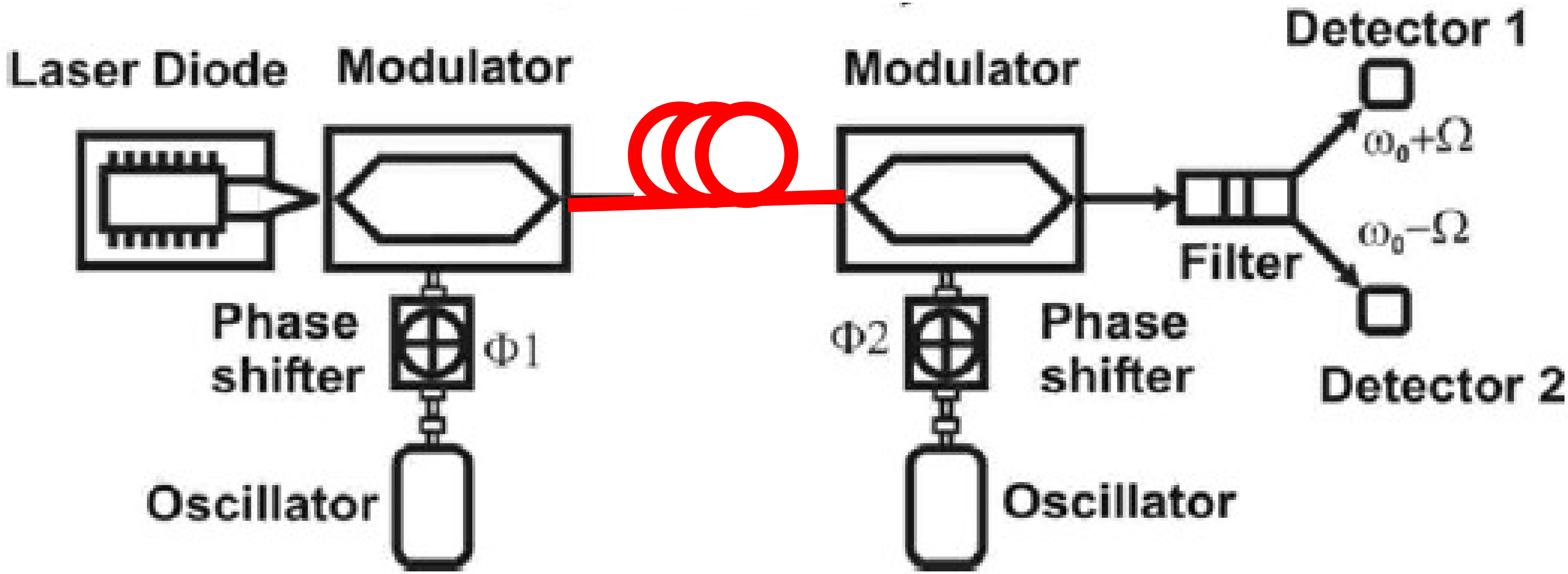


Alice			Bob	
Bit value	ϕ_A	ϕ_B	$\phi_A - \phi_B$	Bit value
0	0	0	0	0
0	0	$\pi/2$	$3\pi/2$	?
1	π	0	π	1
1	π	$\pi/2$	$\pi/2$	?
0	$\pi/2$	0	$\pi/2$	?
0	$\pi/2$	$\pi/2$	0	0
1	$3\pi/2$	0	$3\pi/2$	?
1	$3\pi/2$	$\pi/2$	π	1

Plug&Play System

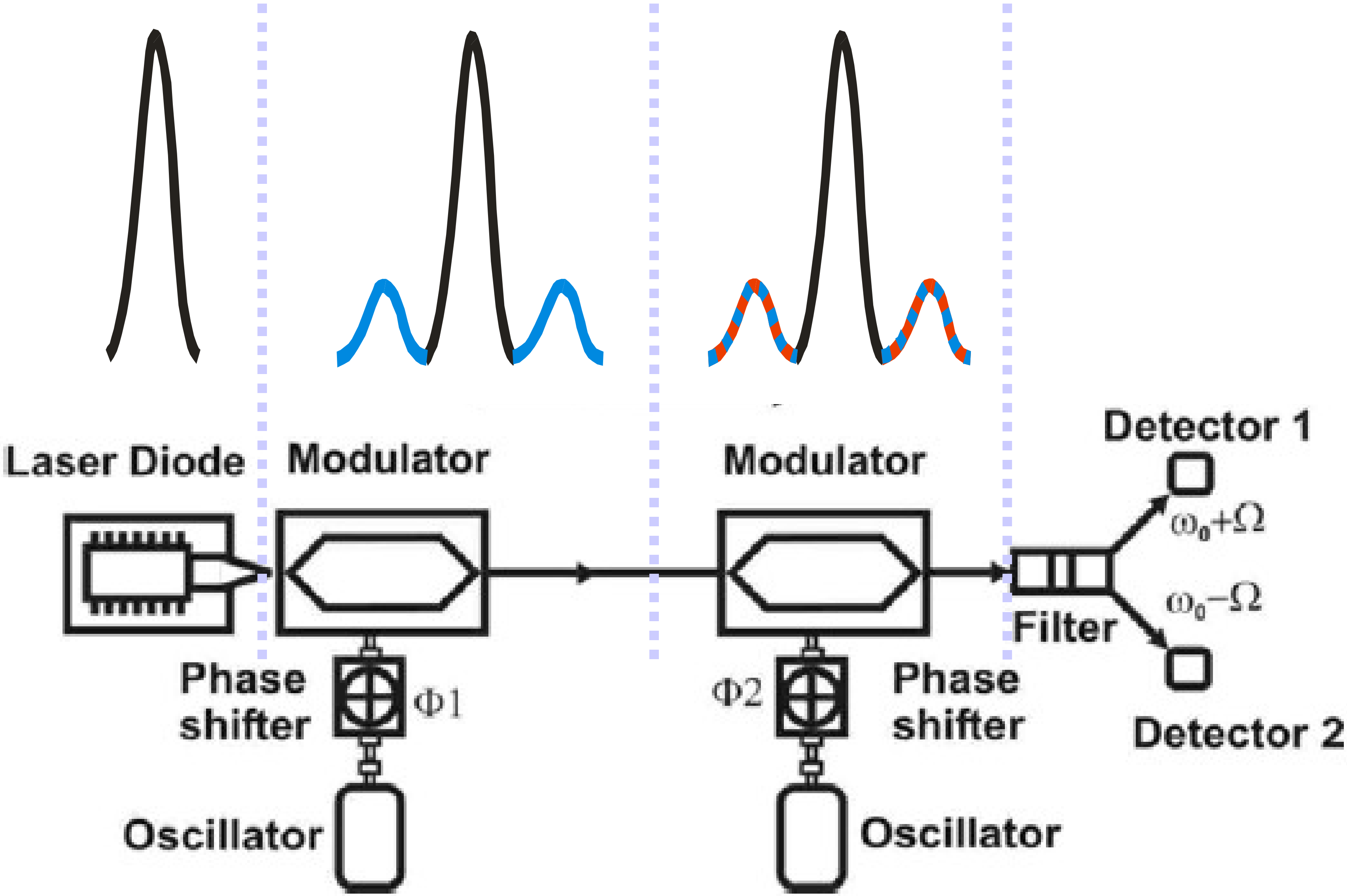


idQuantique



Laser Diode
Modulator
Modulator
Detector 1
$\omega_0+\Omega$
$\omega_0-\Omega$
Filter
Phase shifter
$\Phi1$
$\Phi2$
Phase shifter
Detector 2
Oscillator
Oscillator

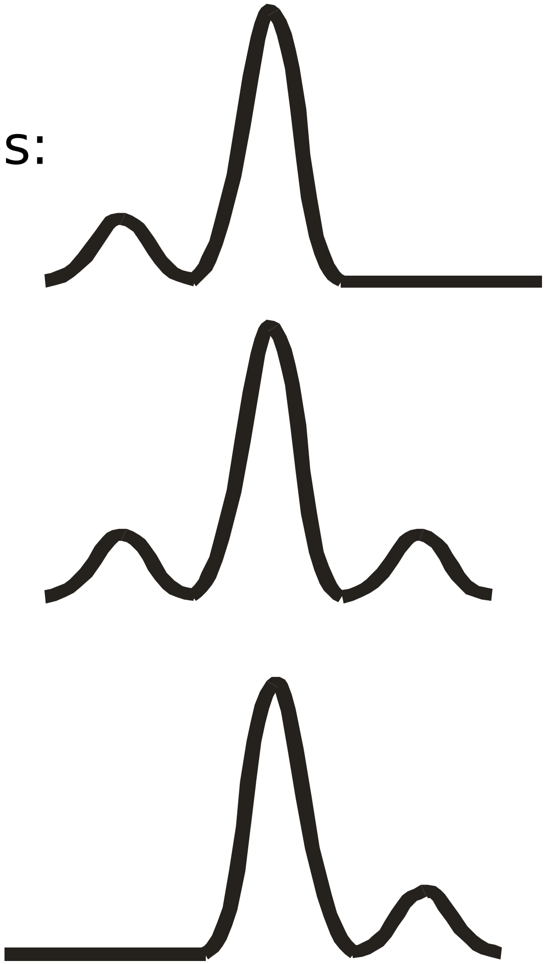
3. FIBER OPTIC SYSTEMS: Frequency Coding



BB84

Alice uses the following RF phases:
- $\pi/2$
- π
- $3\pi/2$

Bob "measures":
- 0
- π

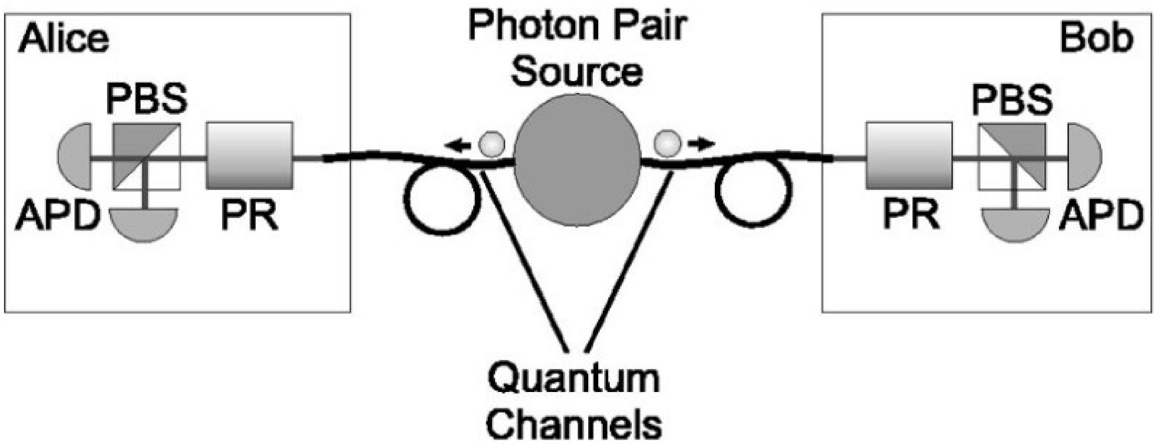


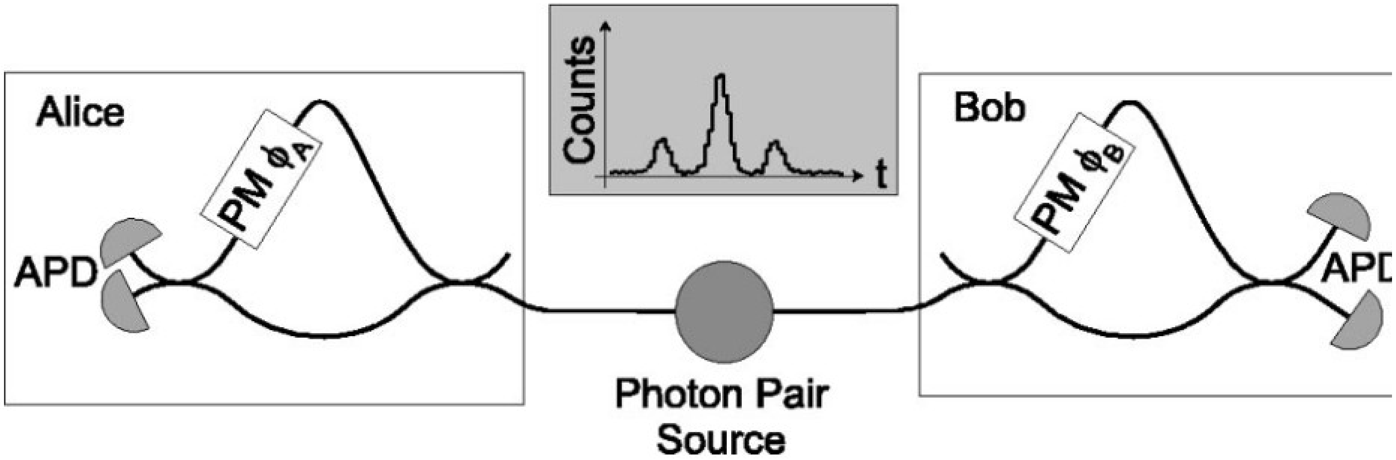
$\Delta\Phi_{A-B}=\pi$

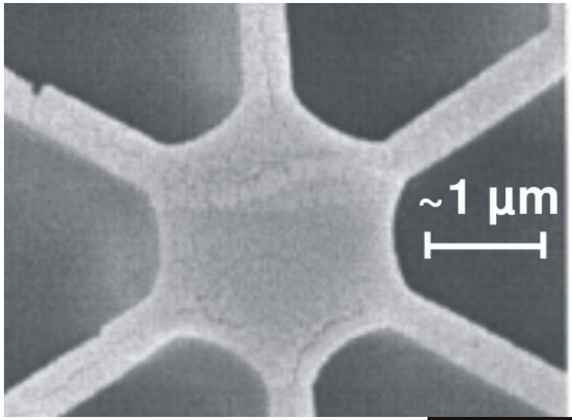
$\Delta\Phi_{A\text{-}B}=\pi/2$

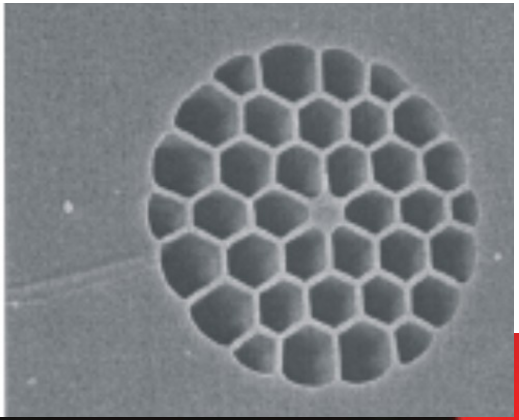
$\Delta\Phi_{A\text{-}B}=0$

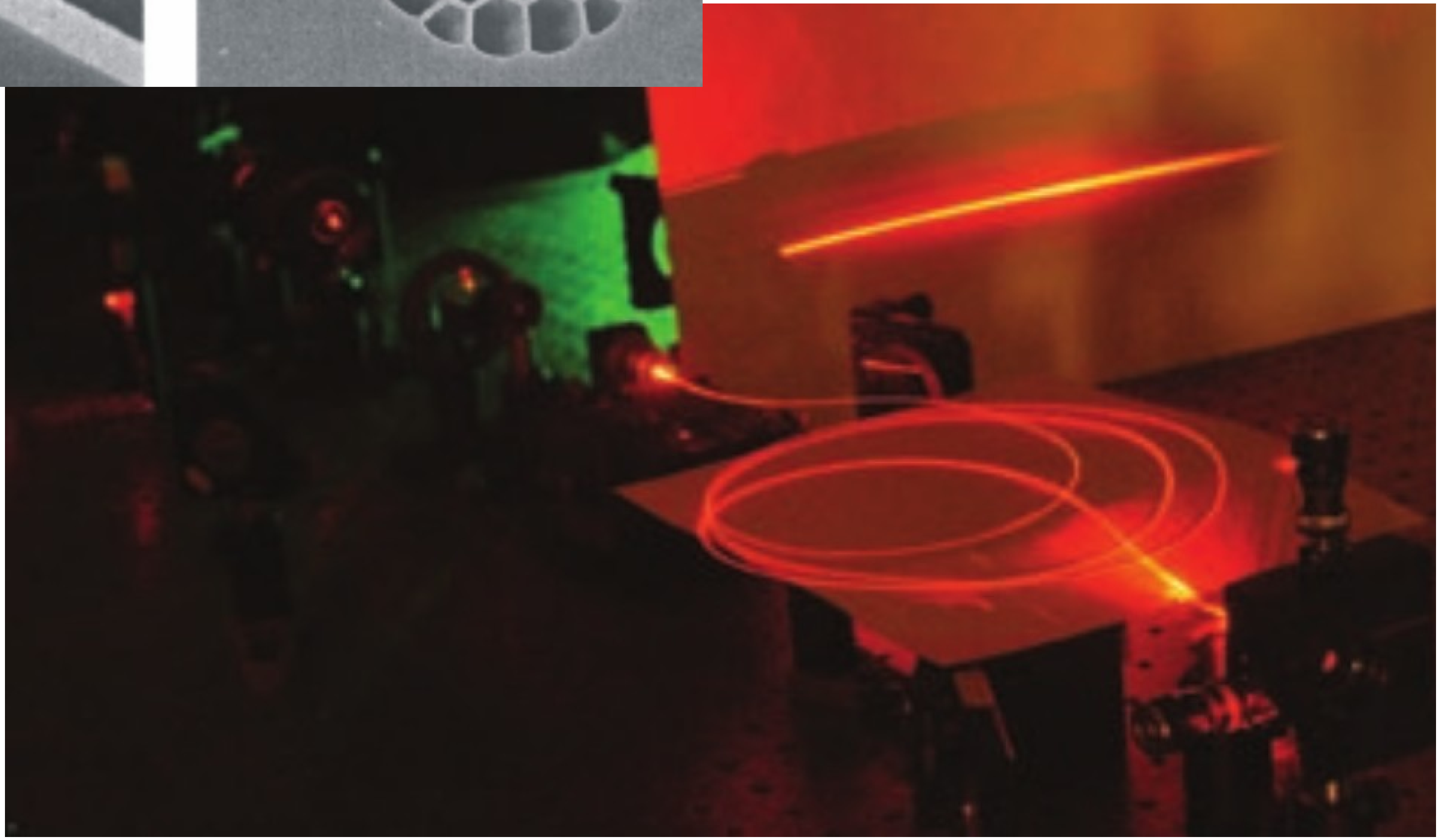
3. FIBER OPTIC SYSTEMS: Entangled Pairs

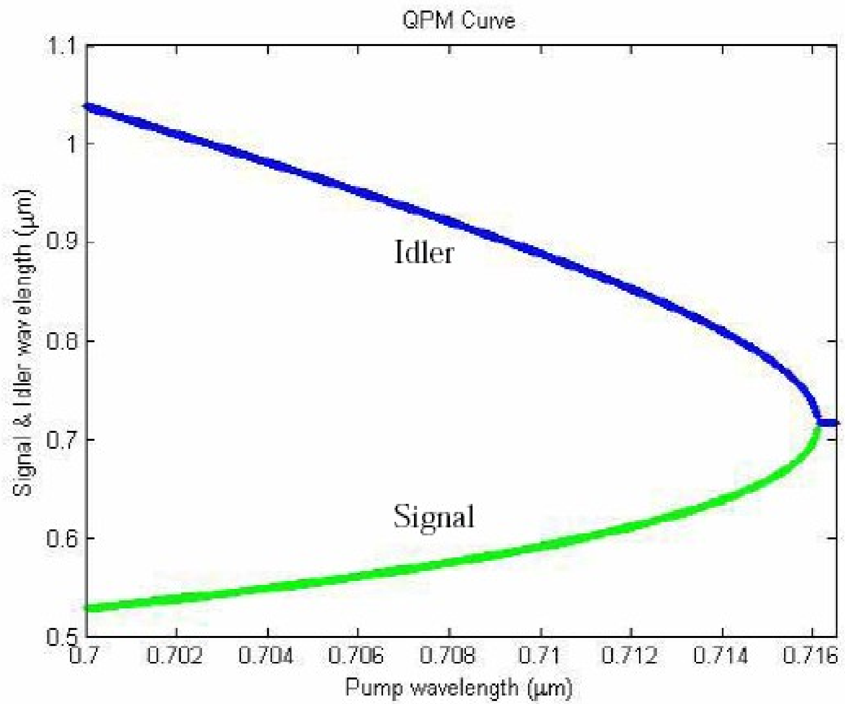


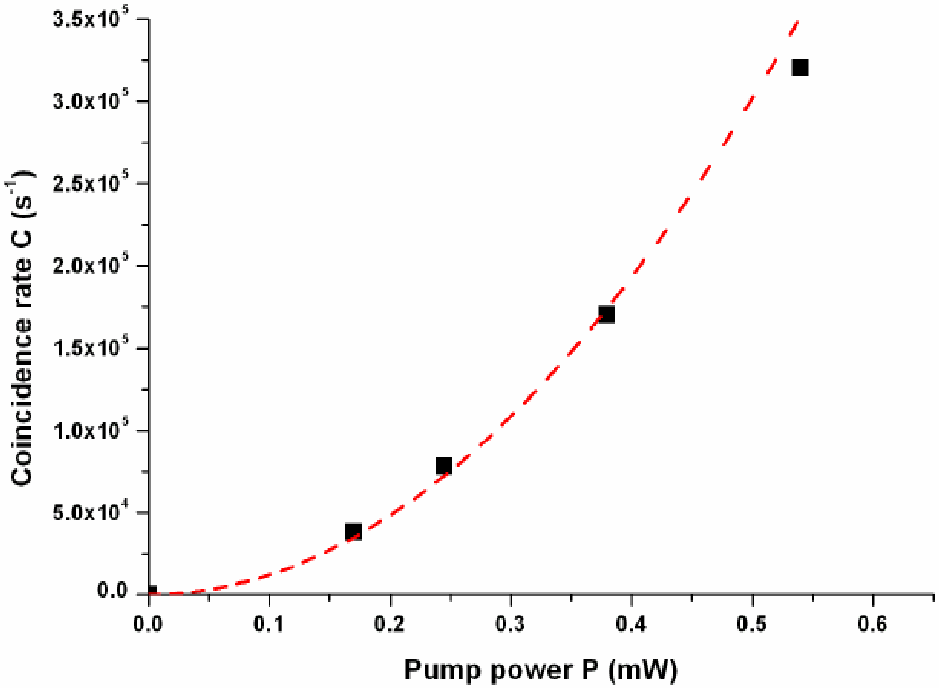



~1 µm

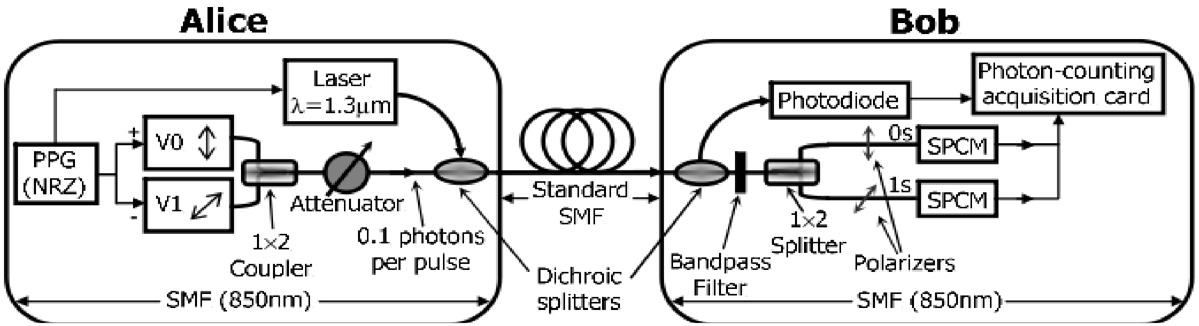








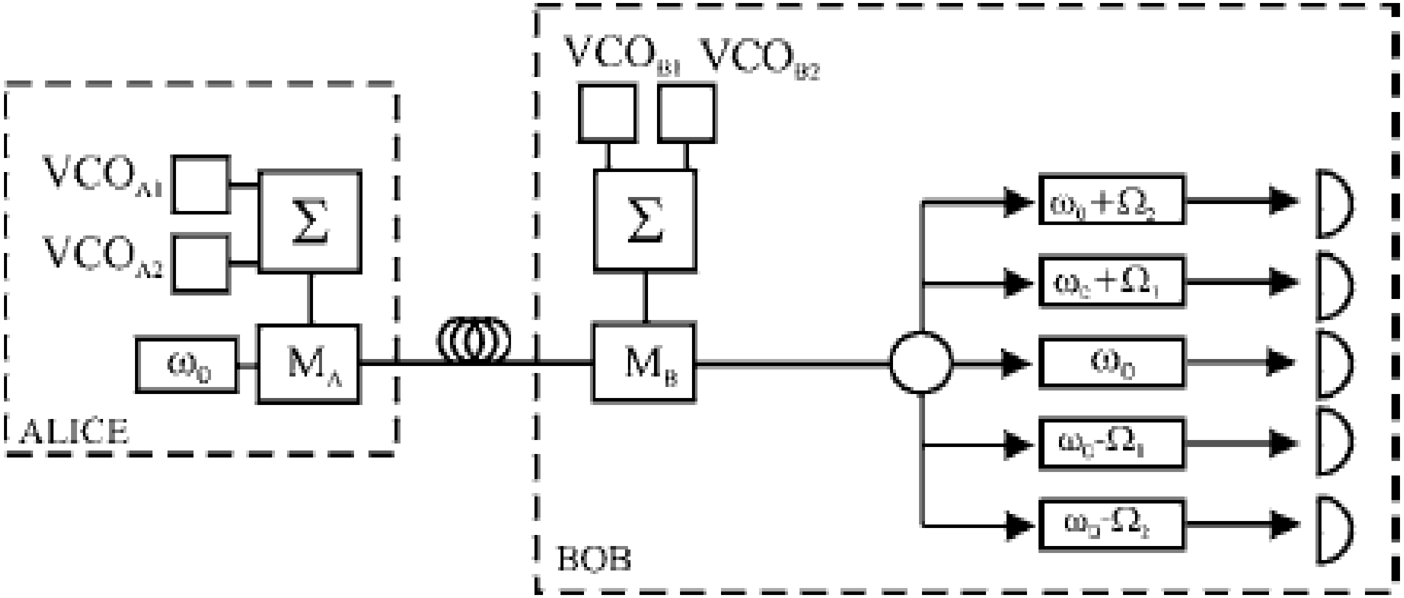
. Fulconis, O. Alibart, W. Wadsworth, P. Russell, and J. Rarity,
"High brightness single mode source of correlated photon pairs
using a photonic crystal fiber,"
Opt. Express 13, 7572-7582 (2005)



* MultiplexIng of the clock signal

* Parallel key distribution in second and third window?

* Parallel key distribution in the same window?

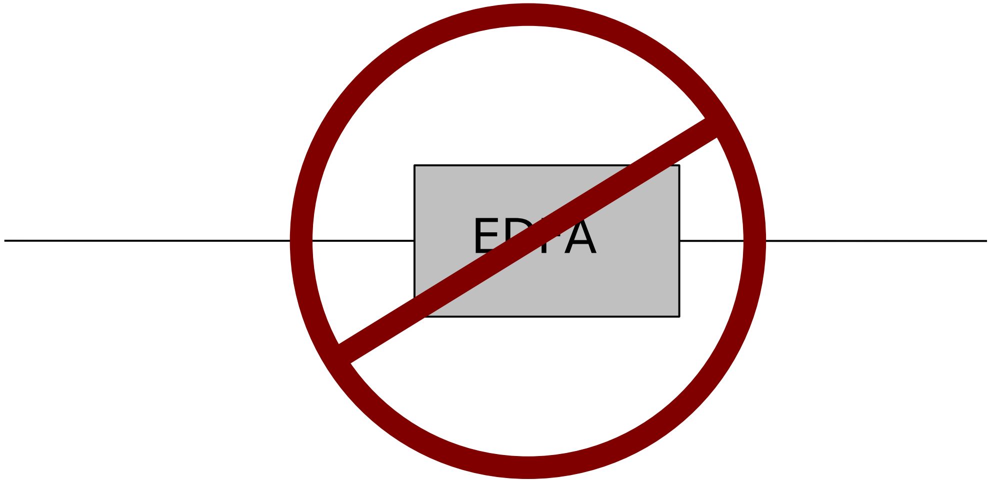


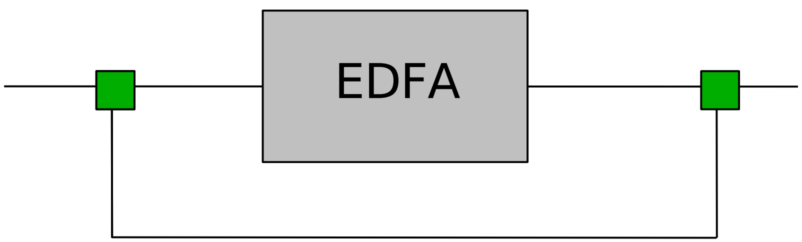
* Channel Multimplexing using SCM

* Parallel key distribution in second and third window

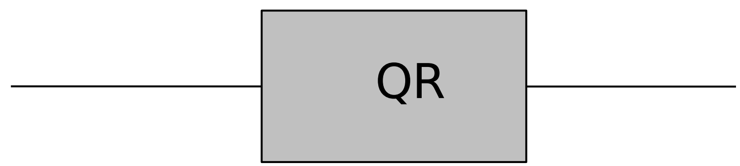
* Parallel key distribution in the same window?
Modified CATV frequency grid?

* Which is the channel limit?



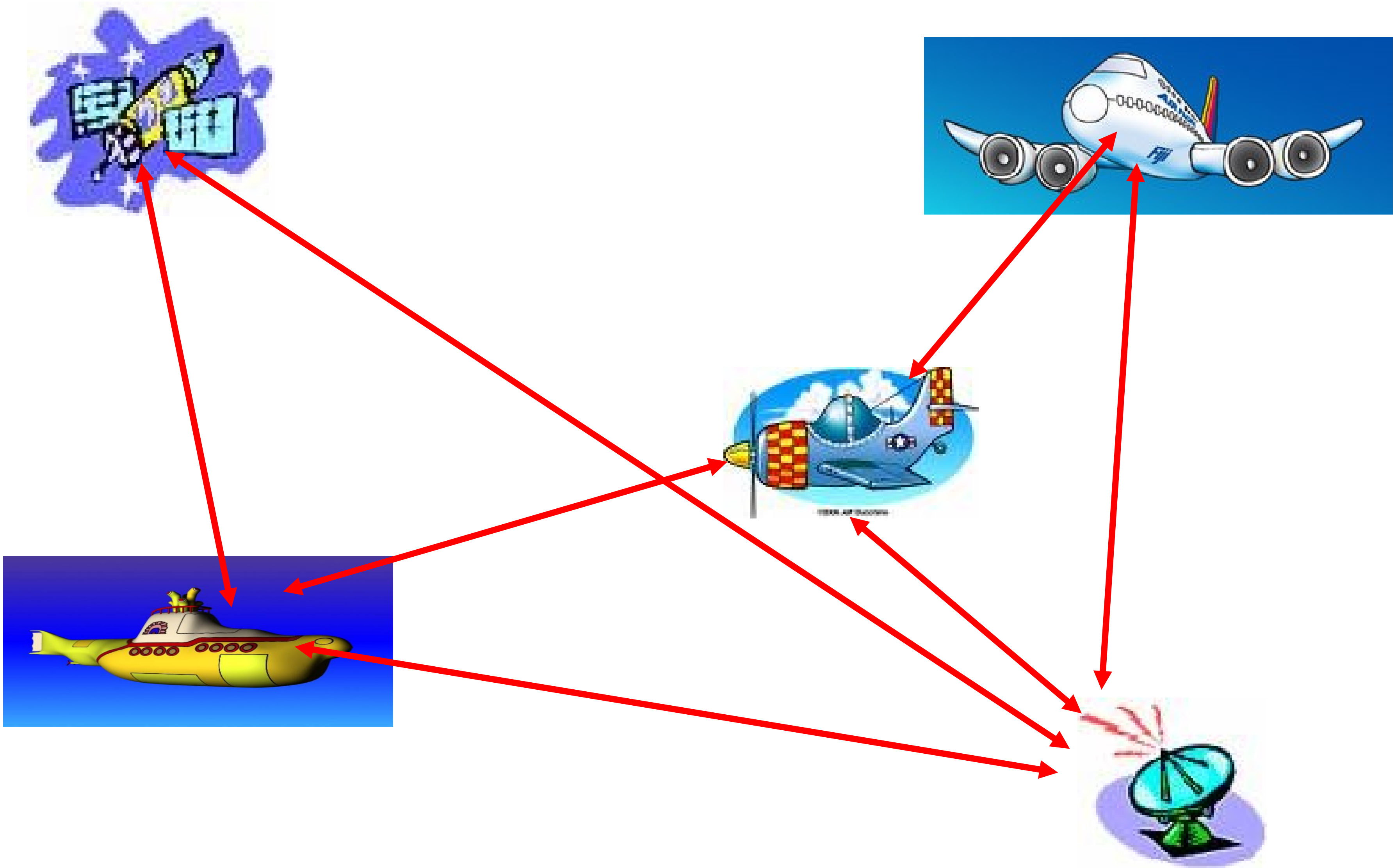


by-pass?

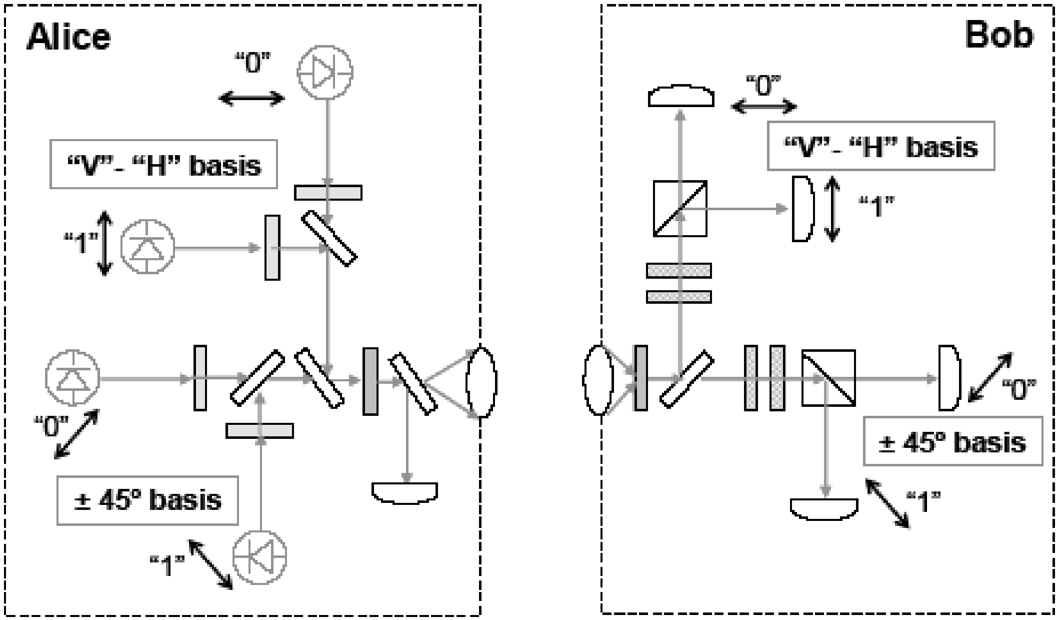


alternatives to EDFAs?

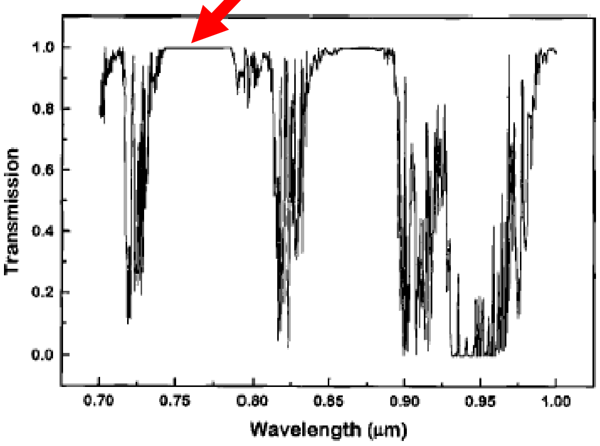
3. Free space Propagation



3. Free space Propagation



APDs



More info @

http://www.gco.upv.es

aortigos@iteam.upv.es

UNIVERSIDAD POLITECNICA DE VALENCIA

Quantum Optical Information Technology