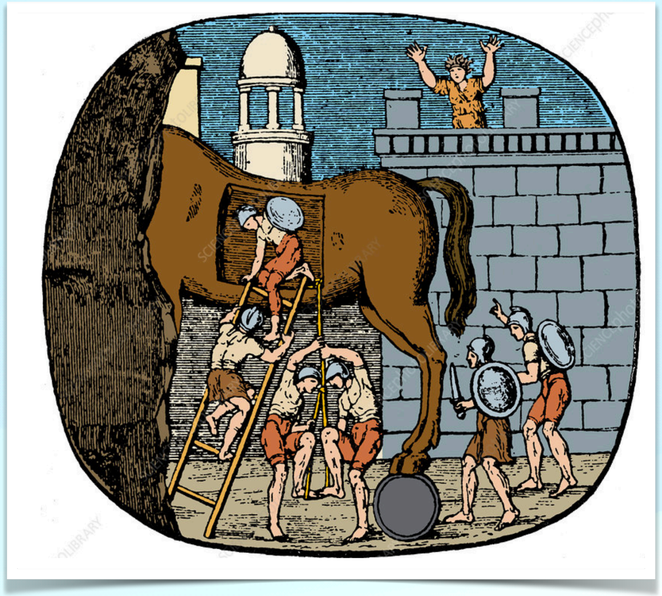


Trojan Horse attack in QKD systems

N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy

Phys. Rev. A 73, 022320 – Published 13 February 2006

Outline of the presentation

- General Trojan horse attacks on QKD systems.

Outline of the presentation

- General Trojan horse attacks on QKD systems.
- Power of such attacks with today’s technology.

Outline of the presentation

- General Trojan horse attacks on QKD systems.
- Power of such attacks with today’s technology.
- **Proposed wayout:** an auxiliary detector that monitors any incoming light.

Outline of the presentation

- General Trojan horse attacks on QKD systems.
- Power of such attacks with today’s technology.
- **Proposed wayout:** an auxiliary detector that monitors any incoming light.
- Such counter-measures can be efficient, ONLY WITH enough additional privacy amplification.

Outline of the presentation

- General Trojan horse attacks on QKD systems.
- Power of such attacks with today’s technology.
- **Proposed wayout:** an auxiliary detector that monitors any incoming light.
- Such counter-measures can be efficient, ONLY WITH enough additional privacy amplification.
- A practical way to reduce the maximal information gain through Trojan horse attacks.

Outline of the presentation

- General Trojan horse attacks on QKD systems.
- Power of such attacks with today's technology.
- **Proposed wayout:** an auxiliary detector that monitors any incoming light.
- Such counter-measures can be efficient, ONLY WITH enough additional **privacy amplification**.
- A practical way to reduce the maximal information gain through Trojan horse attacks.
- This does reduce the security analysis of the **2-way Plug-&-Play system** to those of the standard 1-way systems.

Requirement for QKD: **a Q comm channel, i.e. a channel able to transmit individual quantum systems well enough isolated from the outside world such that the receiver gets them almost unperturbed.**

Introductory remarks

Requirement for QKD: **a Q comm channel, i.e. a channel able to transmit individual quantum systems well enough isolated from the outside world such that the receiver gets them almost unperturbed.**

Practical realisation: **realized with standard telecom optical fifers or with free space in line-of-sight optical channels.**

Introductory remarks

- **The presence of any eavesdropper on the quantum communication channel: detected by the legitimate users**

Introductory remarks

- **The presence of any eavesdropper on the quantum communication channel: detected by the legitimate users**

- **The legitimate users: can upper bound the information that any eavesdropper could gain by eavesdropping the quantum communication channel.**

Introductory remarks

- The presence of any eavesdropper on the quantum communication channel: detected by the legitimate users

- The legitimate users: can upper bound the information that any eavesdropper could gain by eavesdropping the quantum communication channel.

Consequence: The legitimate users can lower bound the amount of privacy amplification they need to apply on their data in order to reduce the eavesdropper's information to an exponentially small value.

Introductory remarks

- The presence of any eavesdropper on the quantum communication channel: detected by the legitimate users

- The legitimate users: can upper bound the information that any eavesdropper could gain by eavesdropping the quantum communication channel.

Consequence: The legitimate users can lower bound the amount of privacy amplification they need to apply on their data in order to reduce the eavesdropper's information to an exponentially small value.

Quantum physics guarantees potential security against any possible attack on the quantum communication channel.

Introductory remarks

Eve: no technological limits (can do everything that quantum physics does not explicitly forbid).

Eve's attacks are not limited to the quantum communication channel.

Eve could attack Alice or Bob’s apparatuses, or she could exploit weaknesses in the actual implementation of abstract QKD.

Introductory remarks

Quantum physics: does not help protecting Alice and Bob’s apparatuses.

Information encoded in a classical physics system: vulnerable to copying and broadcasting.

Alice and Bob's electronics: to be protected by classical means.

Where does the transition from quantum coding to classical coding happen?

An old question: the famous quantum/classical foggy transition.

In a modern setting: To determine what can be protected by quantum means and what has to be protected by classical means.

Not consider this question in this article. Obvious that Alice and Bob's apparatuses need classical protections.

Actual implementations of abstract QKD: uses today's technology (and economical constrains).

Necessarily move somewhat away from the ideal scheme.

consequences of these compromises ???

Some compromises: might render the entire system totally insecure.

Some other compromises: can be proven to maintain absolute security, provided their analyzes are properly taken into account.

Some well implemented compromises do not at all reduce the security of QKD.

Introductory remarks

Example of a compromise: use of weak laser pulses instead of the single-photon sources that are closer to abstract qubits.

First shown to open new eavesdropping strategies.

Introductory remarks

Example of a compromise: use of weak laser pulses instead of the single-photon sources that are closer to abstract qubits.

First shown to open new eavesdropping strategies.

Secure QKD is nevertheless possible, provided the weak intensity of the pulses and the quantum communication channel loss are properly taken into account.

Recently, variations of the basic QKD protocols have been proposed that significantly lighten the conditions for secure QKD using weak laser pulses.

Introductory remarks

Example of a compromise: use of weak laser pulses instead of the single-photon sources that are closer to abstract qubits.

First shown to open new eavesdropping strategies.

Secure QKD is nevertheless possible, provided the weak intensity of the pulses and the quantum communication channel loss are properly taken into account.

Recently, variations of the basic QKD protocols have been proposed that significantly lighten the conditions for secure QKD using weak laser pulses.

Timely to study another unavoidable aspect of QKD: the quantum channel itself is a potentially open door for an eavesdropper into Alice and Bob's apparatuses.

Introductory remarks

Example of a compromise: use of weak laser pulses instead of the single-photon sources that are closer to abstract qubits.

First shown to open new eavesdropping strategies.

Secure QKD is nevertheless possible, provided the weak intensity of the pulses and the quantum communication channel loss are properly taken into account.

Recently, variations of the basic QKD protocols have been proposed that significantly lighten the conditions for secure QKD using weak laser pulses.

Timely to study another unavoidable aspect of QKD: the quantum channel itself is a potentially open door for an eavesdropper into Alice and Bob's apparatuses.

Even if this door is properly designed, Eve could use it precisely at the same time as the legitimate users: Eve could send into Alice and/or Bob's apparatuses light pulses during the (short) times the quantum channel is open

Consider the door as open only during the time when it potentially gives access to some useful Information, the rest of the time the apparatus will merely backscatters a useless signal.

Introductory remarks

Example of a compromise: use of weak laser pulses instead of the single-photon sources that are closer to abstract qubits.

First shown to open new eavesdropping strategies.

Secure QKD is nevertheless possible, provided the weak intensity of the pulses and the quantum communication channel loss are properly taken into account.

Recently, variations of the basic QKD protocols have been proposed that significantly lighten the conditions for secure QKD using weak laser pulses.

Timely to study another unavoidable aspect of QKD: the quantum channel itself is a potentially open door for an eavesdropper into Alice and Bob's apparatuses.

Even if this door is properly designed, Eve could use it precisely at the same time as the legitimate users: Eve could send into Alice and/or Bob's apparatuses light pulses during the (short) times the quantum channel is open

Consider the door as open only during the time when it potentially gives access to some useful Information, the rest of the time the apparatus will merely backscatters a useless signal.

Principle of a Trojan-horse attack

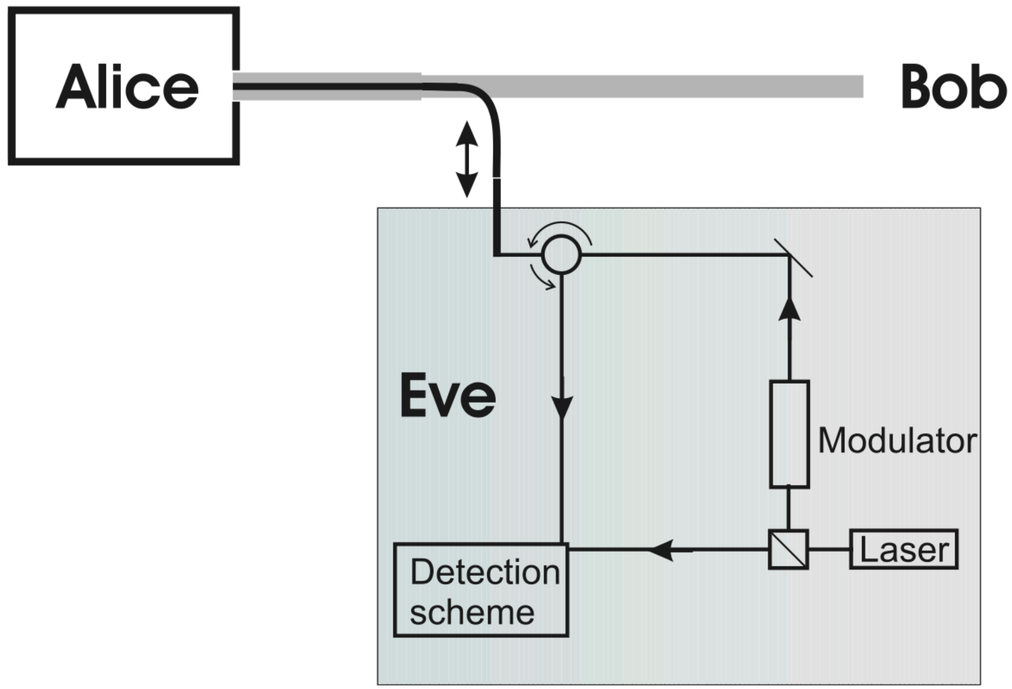


FIG. 1: Principle of a Trojan Horse attack. Eve occupied part of the quantum channel (i.e. the spatial, temporal and frequency modes) to probe Alice's apparatus. Eve uses an auxiliary source, modulates it and analyzes the backscattered signal with a detector. Note that her detection scheme can rely on specificities of her auxiliary source, for instance on its phase. Eve may have to remove part of the legitimate signal, compensating the introduced loss by an improved quantum channel.

Counterfoiling strategies

The system should be designed in such a way that

1. **only light at appropriate wavelength can enter (i.e. filters).**

2. **the "door" should be open only during short times, i.e. the encoding optical components should be active only during short times (i.e. activate phase modulators only when the qubits is there), and**

3. **the amount of reflected light that could be exploited by Eve is bounded by a known value.**

Purpose: to analyze such attacks, known as Trojan horse attacks.

Purpose: to analyze such attacks, known as Trojan horse attacks.

Before the main task, some precursors:

- Reflectometry
- Plug-and-play quantum key distribution setup

Reflectometry

$$\mathrm{dB} = \log_{10} \frac{P_2}{P_1}$$

Every optical element backscatters some amount of any incoming light.

Fibers (about -70dB/m)
Angle-polished connectors (typically -40dB)
Medium for integrated optics components, like phase-modulators ($\approx$ -20 dB) and large for mirrors ($\geq$-1 dB).

Reflectometry

Every optical element backscatters some amount of any incoming light.

$$\mathrm{dB} = \log_{10} \frac{P_2}{P_1}$$

Fibers (about -70dB/m)
Angle-polished connectors (typically -40dB)
Medium for integrated optics components, like phase-modulators ($\approx$ -20 dB) and large for mirrors ($\geq$-1 dB).

Consequence: Every optical apparatus can be examined from the outside by shining into it well controlled light and analyzing the backscattered light.

Reflectometry

Every optical element backscatters some amount of any incoming light.

$$\mathrm{dB} = \log_{10} \frac{P_2}{P_1}$$

Fibers (about -70dB/m)
Angle-polished connectors (typically -40dB)
Medium for integrated optics components, like phase-modulators ($\approx$ -20 dB) and large for mirrors ($\geq$-1 dB).

Consequence: Every optical apparatus can be examined from the outside by shining into it well controlled light and analyzing the backscattered light.

This technique, “reflectometry”, is a standard tool for optical engineers.

Reflectometry

Every optical element backscatters some amount of any incoming light.

$$\mathrm{dB} = \log_{10} \frac{P_2}{P_1}$$

Fibers (about -70dB/m)
Angle-polished connectors (typically -40dB)
Medium for integrated optics components, like phase-modulators ($\approx$ -20 dB) and large for mirrors ($\geq$-1 dB).

Consequence: Every optical apparatus can be examined from the outside by shining into it well controlled light and analyzing the backscattered light.

This technique, “reflectometry”, is a standard tool for optical engineers.

Assumption for security analysis of QKD: an Eve without any technological limit.

Useful to have an idea how the technique works in principle and to illustrate it with today’s technology.

Two approaches to reflectometry

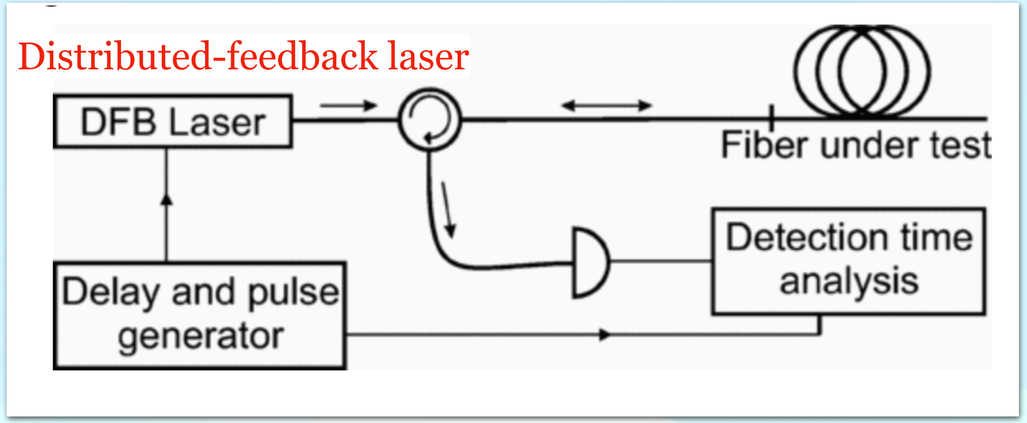
(I) Optical Time Domain Reflectometry (OTDR)

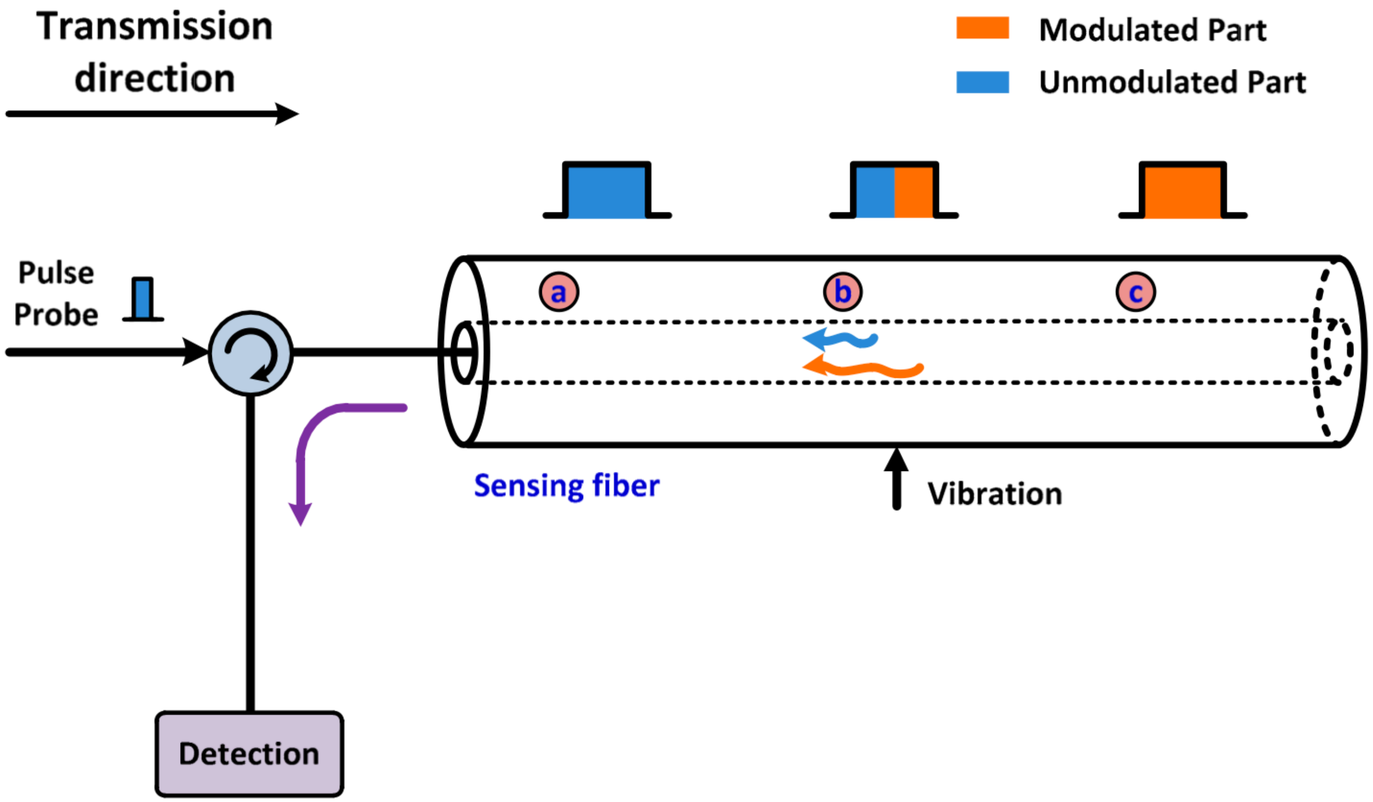
1. Send in short optical pulses.

2. Analyze the backscattered light intensity in function of time.

3. From the known speed of light, the time can be translated into distances.

Very standard tool of optical telecom engineers.





$$E(t) = E_{R1}(t)\exp\{i(2\pi f_c t + \phi_1(t))\} + E_{R0}(t)\exp\{i(2\pi f_c t + \phi_0(t))\}$$

$$I_{\text{direct}} = \left| E_{R1}(t)\exp\{i(2\pi f_c t + \phi_1(t))\} + E_{R0}(t)\exp\{i(2\pi f_c t + \phi_0(t))\} \right|^2$$

$$I_{\text{direct}} = |E_{R1}(t)|^2 + |E_{R0}(t)|^2 + 2E_{R1}(t) \cdot E_{R0}(t)\cos(\phi_1(t) - \phi_0(t))$$

$$I_{\text{coherent}}(t) \propto E_{R1}^2(t) + E_{R0}^2(t) + E_{LO}^2(t) + 2E_{R1}(t)E_{R0}(t)\cos(\phi_1(t) - \phi_0(t))$$

$$+2E_{LO}(t)\cos\theta(t) \cdot \left[E_{R1}(t)\cos(2\pi\Delta ft + \phi_1(t)) + E_{R0}(t)\cos(2\pi\Delta ft + \phi_0(t))\right]$$

$$E_{LO}(t) >> E_{R1}(t),\ \ E_{R2}(t)$$

Two approaches to reflectometry

(II) Optical Frequency Domain Reflectometry (OFDR)

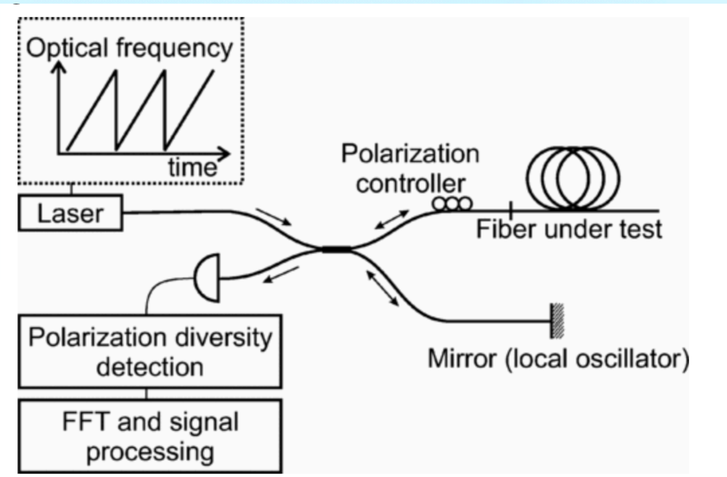
1. Send in coherent cw light while scanning its optical frequency and analyze the spectrum of the backscattered light.

2. Different reflections correspond to different emission times, hence to different optical frequencies.

3. They do thus produce a beat signal.

4. Usually one produces on purpose one relatively large reflection (inside the instrument) which acts as a local oscillator.

5. The frequency of the backscattered signal can be translated into distance by a Fourier transformation.



Two approaches to reflectometry

(II) Optical Frequency Domain Reflectometry (OFDR)

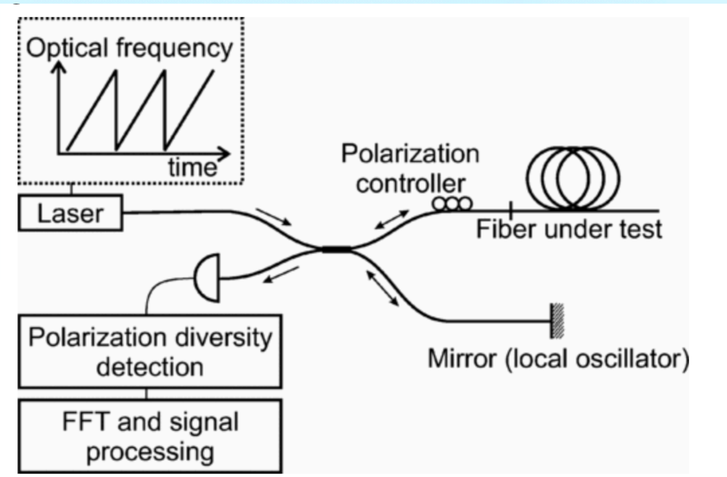
1. Send in coherent cw light while scanning its optical frequency and analyze the spectrum of the backscattered light.

2. Different reflections correspond to different emission times, hence to different optical frequencies.

3. They do thus produce a beat signal.

4. Usually one produces on purpose one relatively large reflection (inside the instrument) which acts as a local oscillator.

5. The frequency of the backscattered signal can be translated into distance by a Fourier transformation.



Not yet as standard as OTDRs, but, thanks to its heterodyne detection scheme, it holds the potential of a much larger sensitivity and dynamical range.

Main drawback of today's OFDRs compared to OTDRs: **their limited distance range, due to the finite coherence length of the cw laser.**

THEN WHY TO TALK ABOUT IT? **As Eve has no technological limits, the potential of Trojan horse attacks using this technique has been shown.**

A point to remember: **only an illustration, clearly the counter measure by Alice and Bob should take into account reflectometry techniques beyond today's technique.**

Second precursor: Plug-and-play QKD systems

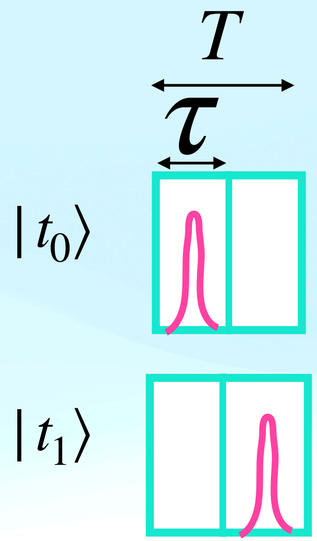
RESEARCH ARTICLE | FEBRUARY 17 1997

“Plug and play” systems for quantum cryptography

A. Muller; T. Herzog; B. Huttner; ... et. al

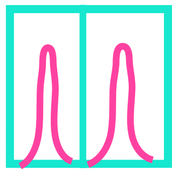
Appl. Phys. Lett. 70, 793–795 (1997)
https://doi.org/10.1063/1.118224

Precursor: Schematic for experimental implementation
Time encoding based BB 84 protocol



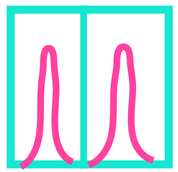
$$|f_0\rangle = \frac{1}{\sqrt{2}}\left(|t_0\rangle + |t_1\rangle\right)$$

0 0

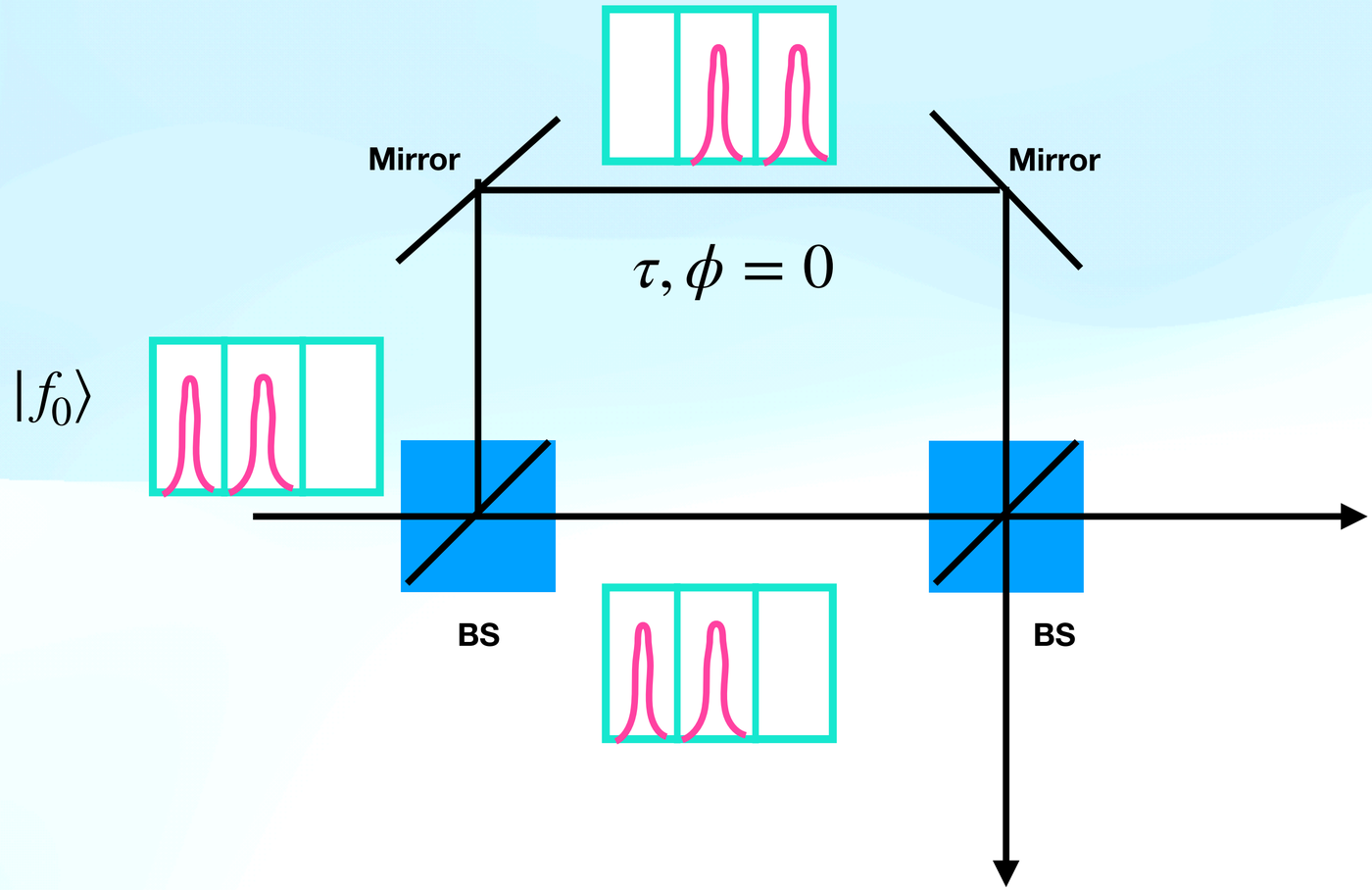


$$|f_1\rangle = \frac{1}{\sqrt{2}}\left(|t_0\rangle - |t_1\rangle\right)$$

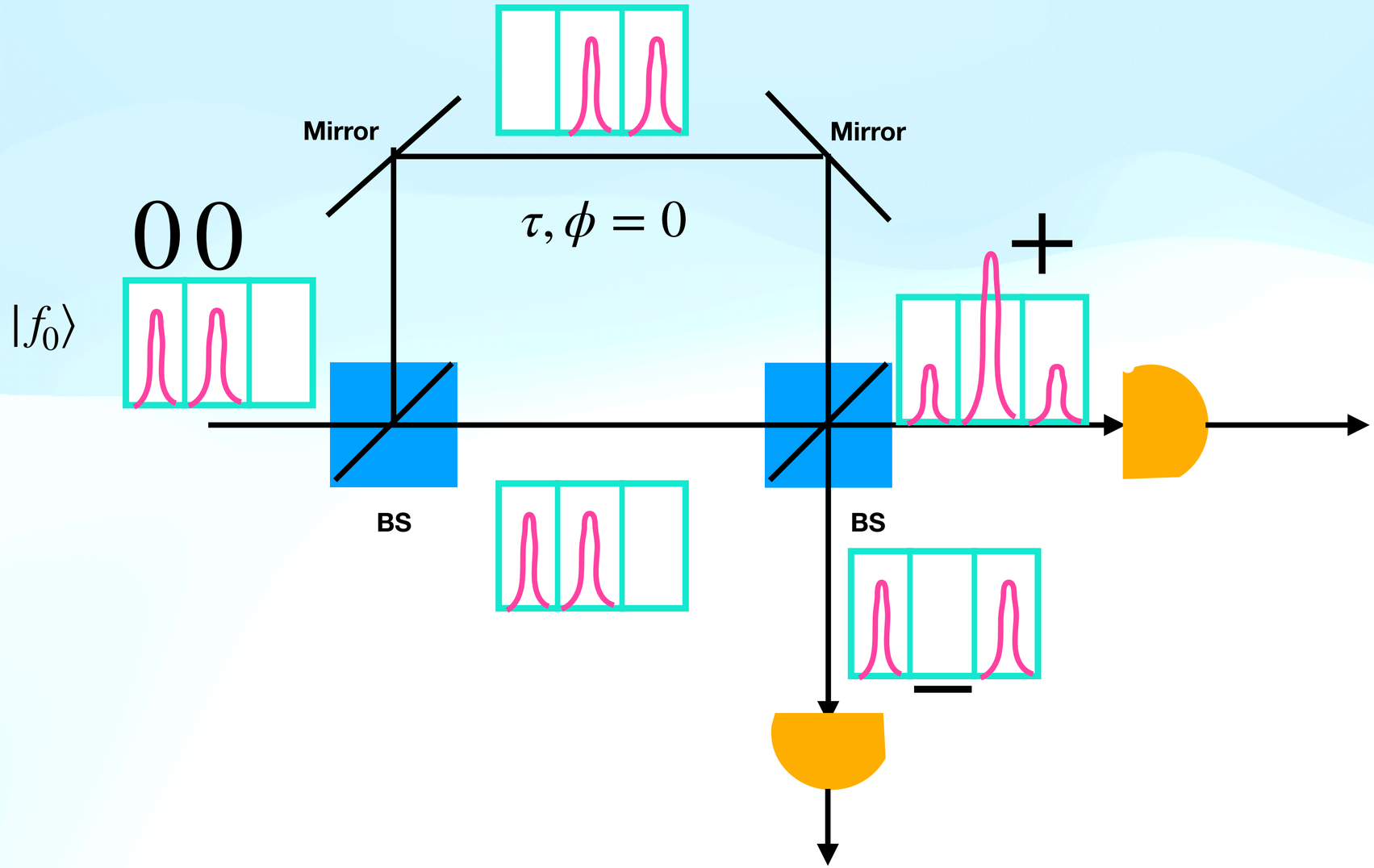
0 π



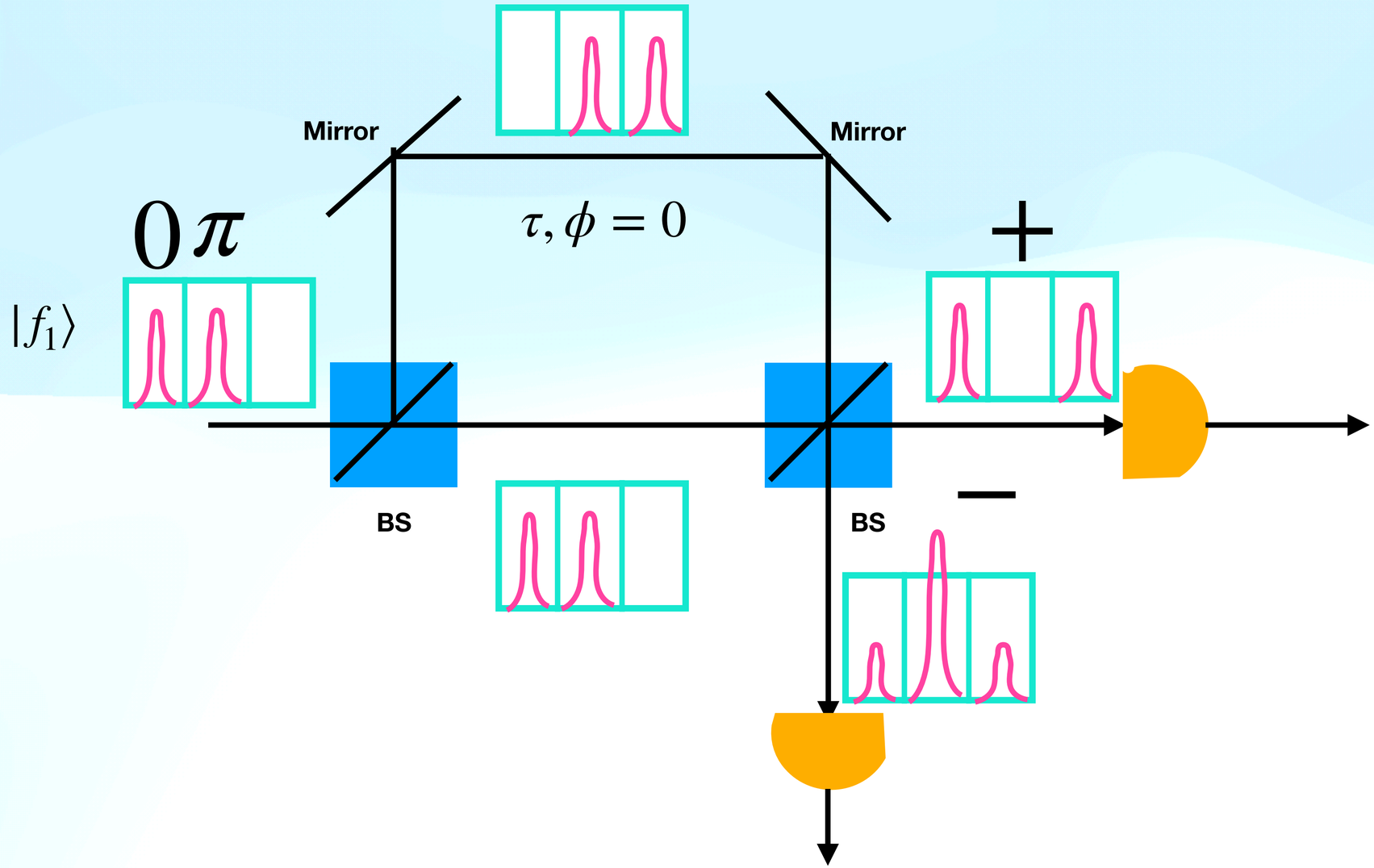
Precursor: Schematic for experimental implementation
Time encoding based BB 84 protocol



Precursor: Schematic for experimental implementation
Time encoding based BB 84 protocol



Precursor: Schematic for experimental implementation
Time encoding based BB 84 protocol



A critique of interferometric systems for quantum cryptography (BB84)

Interferometric QKD systems: usually based on a double Mach–Zehnder interferometer, one side for Alice and one for Bob.

“Plug and play” systems for quantum cryptography A. Muller; T. Herzog; B. Huttner; ... et. al Appl. Phys. Lett. 70, 793–795 (1997)

A critique of interferometric systems for quantum cryptography (BB84)

Interferometric QKD systems: usually based on a double Mach–Zehnder interferometer, one side for Alice and one for Bob.

Implement time-multiplexing, as both interfering pulses follow the same path between Alice and Bob, with some time delay.

“Plug and play” systems for quantum cryptography A. Muller; T. Herzog; B. Huttner; ... et. al Appl. Phys. Lett. 70, 793–795 (1997)

A critique of interferometric systems for quantum cryptography (BB84)

Interferometric QKD systems: usually based on a double Mach–Zehnder interferometer, one side for Alice and one for Bob.

Implement **time-multiplexing**, as both interfering pulses follow the same path between Alice and Bob, with some time delay.

However, the pulses do follow different paths within both Alice's and Bob's interferometers.

"Plug and play" systems for quantum cryptography A. Muller; T. Herzog; B. Huttner; ... et. al
Appl. Phys. Lett. 70, 793–795 (1997)

A critique of interferometric systems for quantum cryptography (BB84)

Interferometric QKD systems: usually based on a double Mach–Zehnder interferometer, one side for Alice and one for Bob.

Implement time-multiplexing, as both interfering pulses follow the same path between Alice and Bob, with some time delay.

However, the pulses do follow different paths within both Alice's and Bob's interferometers.

Conditions for a good interference: (I) both users need to have identical interferometers, (II) the same coupling ratios in each arm and (III) the same path lengths, and (IV) also need to keep them stable within a few tens of nm during a transmission.

"Plug and play" systems for quantum cryptography A. Muller; T. Herzog; B. Huttner; ... et. al Appl. Phys. Lett. 70, 793–795 (1997)

A critique of interferometric systems for quantum cryptography (BB84)

Interferometric QKD systems: usually based on a double Mach–Zehnder interferometer, one side for Alice and one for Bob.

Implement time-multiplexing, as both interfering pulses follow the same path between Alice and Bob, with some time delay.

However, the pulses do follow different paths within both Alice's and Bob's interferometers.

Conditions for a good interference: (I) both users need to have identical interferometers, (II) the same coupling ratios in each arm and (III) the same path lengths, and (IV) also need to keep them stable within a few tens of nm during a transmission.

Challenges: Optical components like phase modulators are polarization dependent. Polarization control necessary both in the transmission line and within each interferometer.

"Plug and play" systems for quantum cryptography A. Muller; T. Herzog; B. Huttner; ... et. al
Appl. Phys. Lett. 70, 793–795 (1997)

How to remove/ minimise them??
Use less number of paths

A new interferometric system based on time-multiplexing

- The interfering pulses now following exactly the same spatial path, albeit with a small time delay.

A new interferometric system based on time-multiplexing: demands

- The interfering pulses should follow exactly the same spatial path, albeit with a small time delay.
- Consequence: Does not require any path length control between the various paths.

A new interferometric system based on time-multiplexing

- The interfering pulses should follow exactly the same spatial path, albeit with a small time delay.
- Consequence: Does not require any path length control between the various paths.
- All pulses reflected back at the end of the fibers.
- Use of Faraday mirrors instead of regular mirrors: suppresses all birefringence effects and polarization dependent losses occurring during the transmission.

A new interferometric system based on time-multiplexing

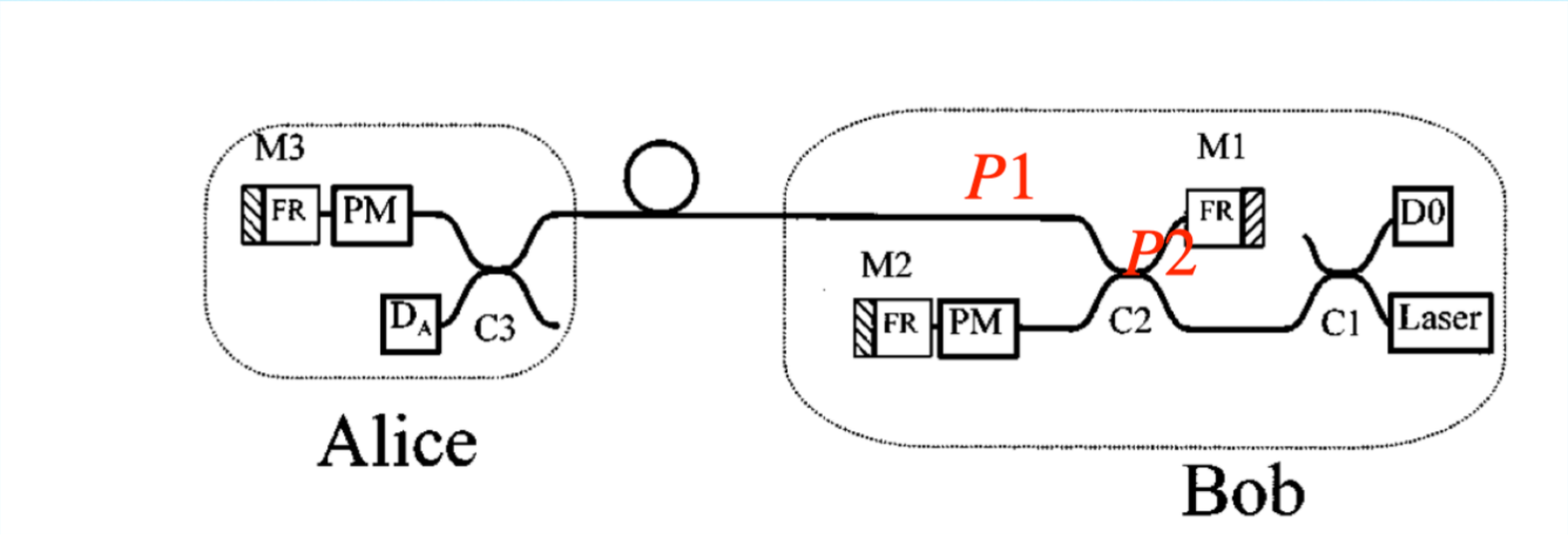
- The interfering pulses should follow **exactly the same spatial path**, albeit with a small time delay.
- **Consequence:** Does not require any path length control between the various paths.
- All pulses reflected back at the end of the fibers.
- **Use of Faraday mirrors instead of regular mirrors:** suppresses all birefringence effects and polarization dependent losses occurring during the transmission.
- No polarization control required.
- **Essence:** with this system, Alice and Bob could exchange their cryptographic keys through standard telecom systems, with no need for lengthy adjustments.

A new interferometric system based on time-multiplexing

- The interfering pulses should follow exactly the same spatial path, albeit with a small time delay.
- Consequence: Does not require any path length control between the various paths.
- All pulses reflected back at the end of the fibers.
- Use of Faraday mirrors instead of regular mirrors: suppresses all birefringence effects and polarization dependent losses occurring during the transmission.
- No polarization control required.
- Essence: with this system, Alice and Bob could exchange their cryptographic keys through standard telecom systems, with no need for lengthy adjustments.
- They would be provided with a sending kit and a receiving kit, and could simply plug them in at the end of the fiber, synchronize their signals, and start the exchange.

This is why it is a “plug and play” system.

Plug-and-play setup: Details

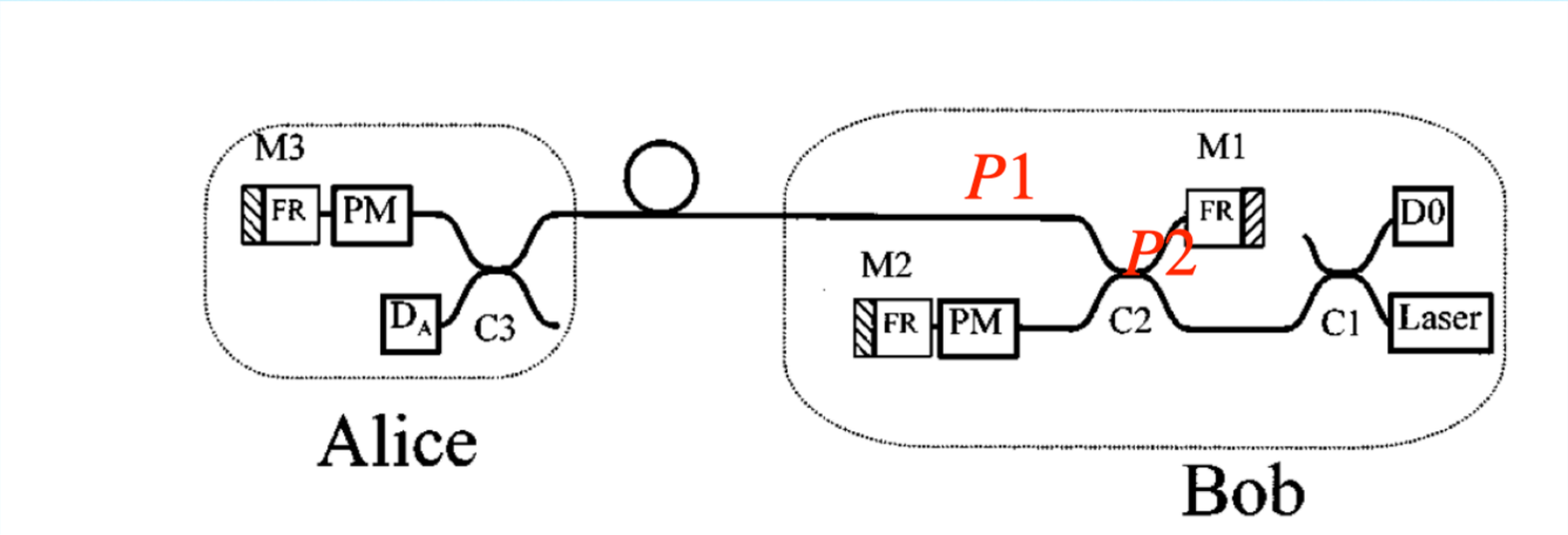


Bob: initiates the transmission by sending a short laser pulse towards Alice.

Pulse arriving in C2: split into two parts: (I) **P1:** goes directly towards Alice
(II) **P2:** first delayed by one bounce in the M2-M1 delay line.

P1 and P2, travel down the fiber to Alice.

Plug-and-play setup: Details



Bob: initiates the transmission by sending a short laser pulse towards Alice.

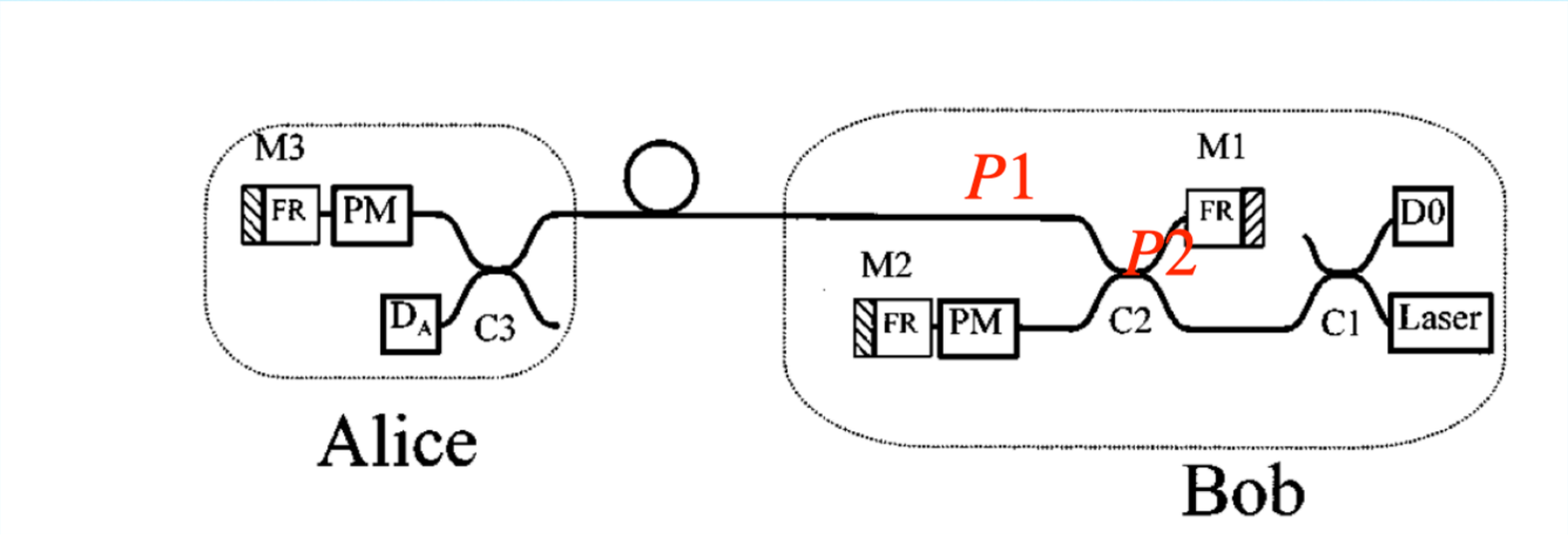
Pulse arriving in C2: split into two parts: (I) **P1:** goes directly towards Alice
(II) **P2:** first delayed by one bounce in the M2-M1 delay line.

P1 and P2, travel down the fiber to Alice.

Bit encoding: Alice lets P1 be reflected by M3, but modulates the phase of P2.

Detection on Bob's side: By delaying part of P1 in the same M1-M2 delay line using also another PM, this time on P1, and looking at the interference with P2.

Plug-and-play setup: Details



Bob: initiates the transmission by sending a short laser pulse towards Alice.

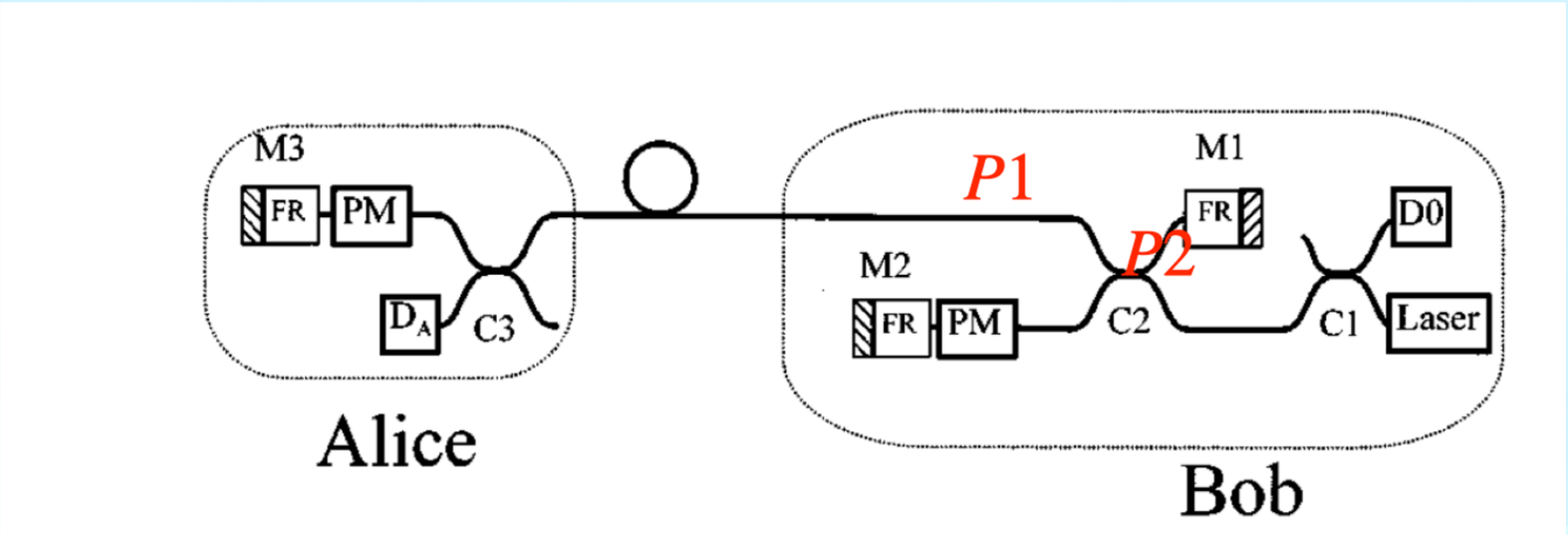
Pulse arriving in C2: split into two parts: (I) **P1:** goes directly towards Alice
(II) **P2:** first delayed by one bounce in the M2-M1 delay line.

P1 and P2, travel down the fiber to Alice.

Bit encoding: Alice lets P1 be reflected by M3, but modulates the phase of P2.

Detection on Bob's side: By delaying part of P1 in the same M1-M2 delay line using also another PM, this time on P1, and looking at the interference with P2.

Plug-and-play setup: Details



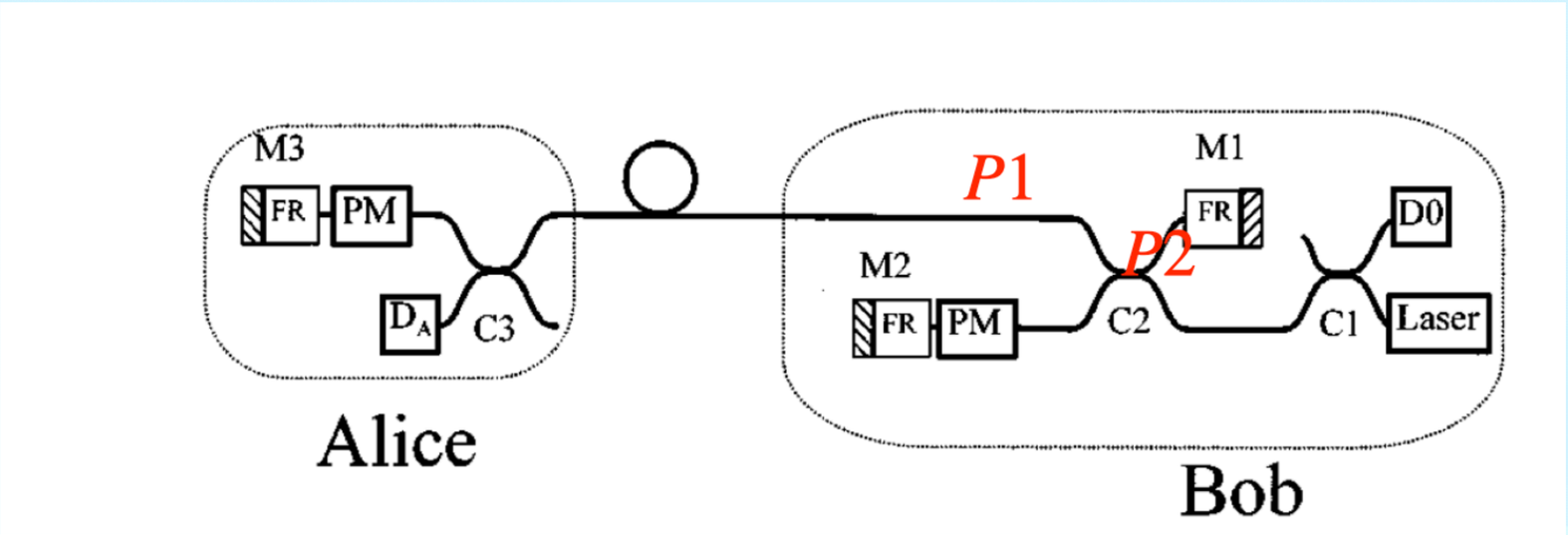
Bit encoding:

If the both PMs are off, the interference is constructive (the two pulses follow exactly the same path).

Destructive interference is obtained when $\phi_A - \phi_B = \pi$,

ϕ_A and ϕ_B : total phase shifts introduced by Alice and Bob, respectively.

Plug-and-play setup: Details



$\phi_A - \phi_B = \pi$ No light detected at D0.

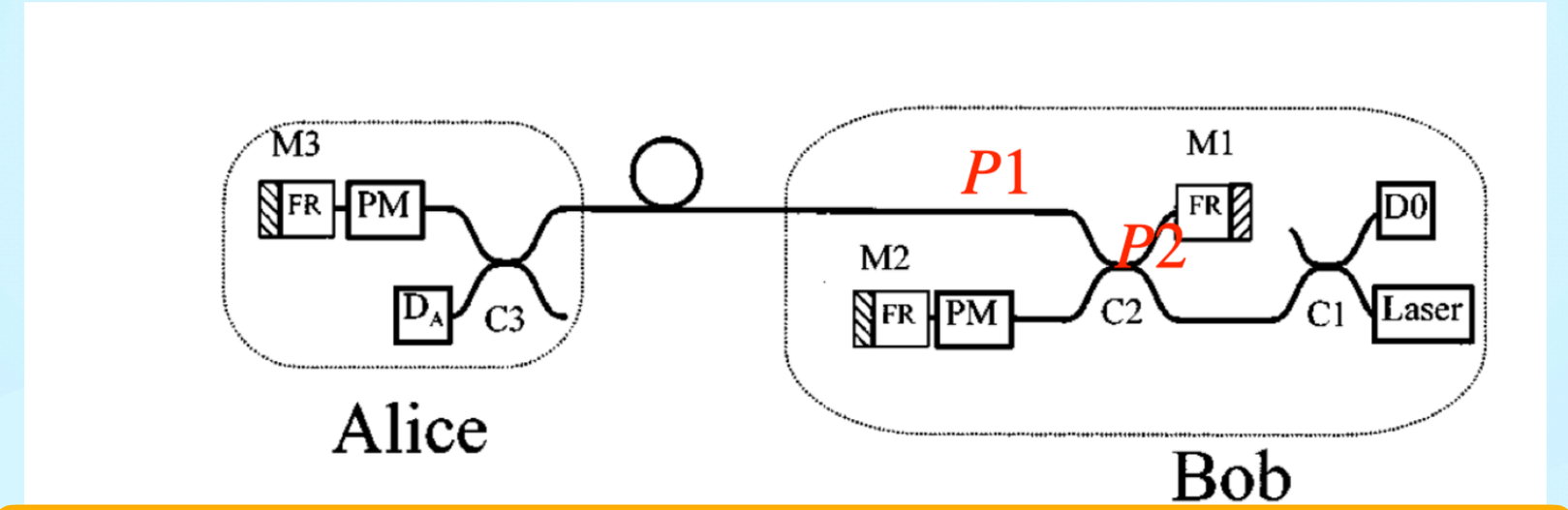
The relative phase setup modulates the intensity in D0, and thus can be used to transfer information from Alice to Bob.

Attractive features of setup: (I) The interferometer is automatically aligned both pulses are delayed by the same delay line, and that the visibility of the fringes is independent of the transmission/reflection coefficients of C2.

A large fraction of the light does not follow these two paths, but is split differently at the various couplers e.g., keeps oscillating a few times between M1-M2 or M1-M3 before leaving towards D0.

These pulses will eventually arrive in D0, but at a different time, and will be easily discriminated. Therefore, they do not reduce the visibility.

Plug-and-play setup: Details



This setup would work perfectly well for ideal fibers, with no birefringence.

In this case no light is detected at D0.

This shows that the relative phase setup modulates the intensity in D0, and thus can be used to transfer information from Alice to Bob.

The first attractive features of this setup are that the interferometer is automatically aligned both pulses are delayed by the same delay line, and that the visibility of the fringes is independent of the transmission/reflection coefficients of C2.

Of course, a large fraction of the light does not follow these two paths, but is split differently at the various couplers ~e.g., keeps oscillating a few times between M1-M2 or M1-M3 before leaving towards D0.

These pulses will eventually arrive in D0, but at a different time, and will be easily discriminated. Therefore, they do not reduce the visibility.

Plug-and-play setup: what if polarisation is not maintained?

All existing optical fibers have birefringence and polarization couplings, which will modify randomly the state of polarization of the light, and may lead to a reduction in the visibility of the interference.

What to do??

Plug-and-play setup: what if polarisation is not maintained?

However, all existing optical fibers have birefringence and polarization couplings, which will modify randomly the state of polarization of the light, and may lead to a reduction in the visibility of the interference.

What to do??

In order to preserve interference, replace the mirrors by Faraday mirrors.

Faraday mirror: an ordinary mirror, glued on a Faraday rotator, which rotates the polarization by 45°.

Plug-and-play setup: what if polarisation is not maintained?

This setup would work perfectly well for ideal fibers, with no birefringence.

However, all existing optical fibers have birefringence and polarization couplings, which will modify randomly the state of polarization of the light, and may lead to a reduction in the visibility of the interference.

What to do??

In order to preserve interference, we replace the mirrors by so-called Faraday mirrors.

Faraday mirror: an ordinary mirror, glued on a Faraday rotator, which rotates the polarization by 45°.

The effect of a FM is to transform any polarization state into its orthogonal.

Consequence: a FM automatically compensates any birefringence effect in the fiber: the state going out of the fiber is alway orthogonal to the incoming state.

Plug-and-play setup: what if polarisation is not maintained?

This setup would work perfectly well for ideal fibers, with no birefringence.

However, all existing optical fibers have birefringence and polarization couplings, which will modify randomly the state of polarization of the light, and may lead to a reduction in the visibility of the interference.

What to do??

In order to preserve interference, we replace the mirrors by so-called Faraday mirrors.

Faraday mirror: an ordinary mirror, glued on a Faraday rotator, which rotates the polarization by 45°.

The effect of a FM is to transform any polarization state into its orthogonal.

Consequence: a FM automatically compensates any birefringence effect in the fiber: the state going out of the fiber is alway orthogonal to the incoming state.

Replacing the ordinary mirrors M1 and M2 by FMs i.e., adding the FRs, thus ensures that the two pulses P1 and P2 have the same polarization, irrespective of birefringence effects in the delay line M1-M2.

Use of an extra FM in M3 enables one to compensate for the polarization dependence of the PM.

Plug-and-play setup: what if polarisation is not maintained?

This setup would work perfectly well for ideal fibers, with no birefringence.

However, all existing optical fibers have birefringence and polarization couplings, which will modify randomly the state of polarization of the light, and may lead to a reduction in the visibility of the interference.

What to do??

In order to preserve interference, we replace the mirrors by so-called Faraday mirrors.

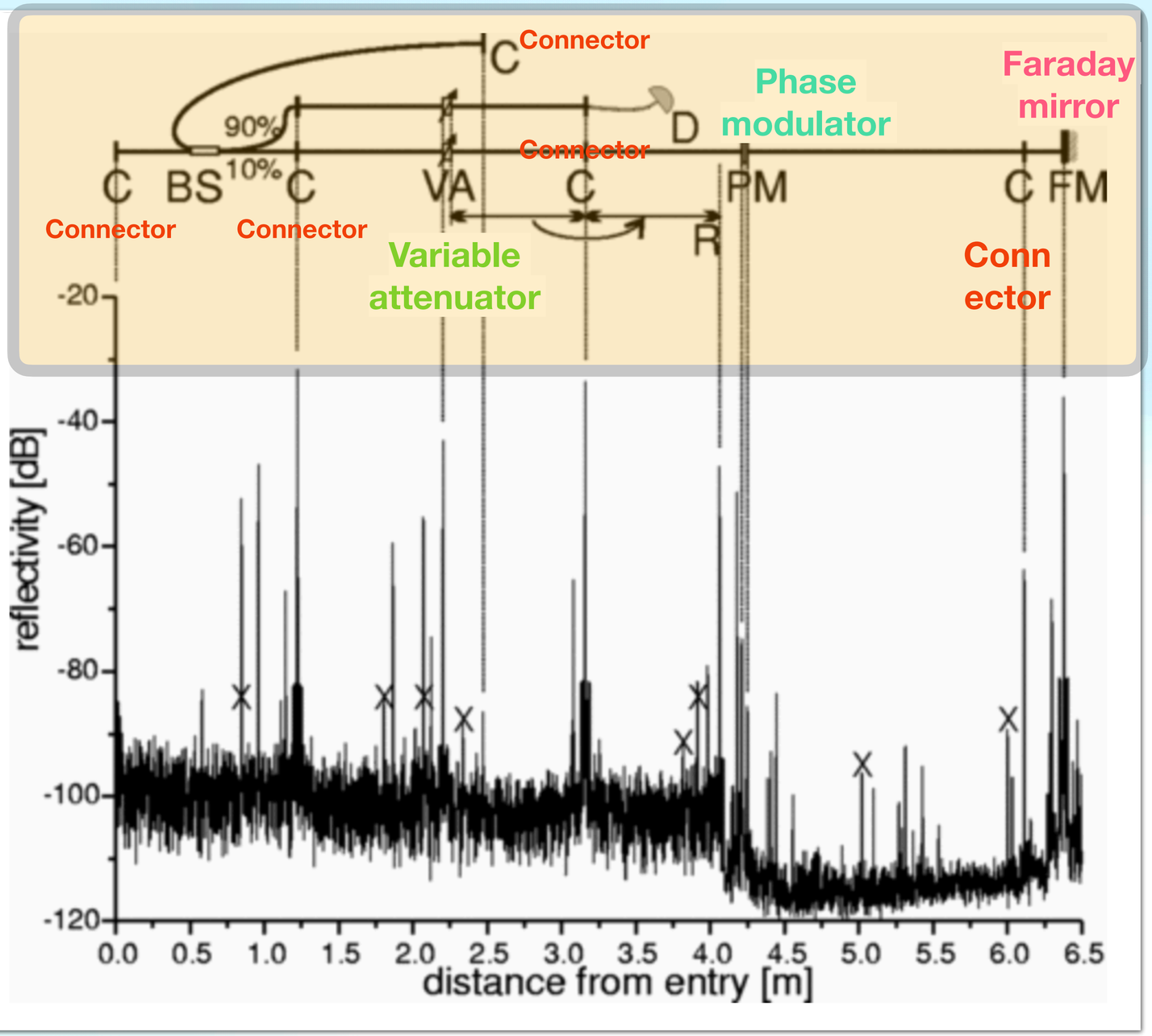
Faraday mirror: an ordinary mirror, glued on a Faraday rotator, which rotates the polarization by 45°.

The effect of a FM is to transform any polarization state into its orthogonal.

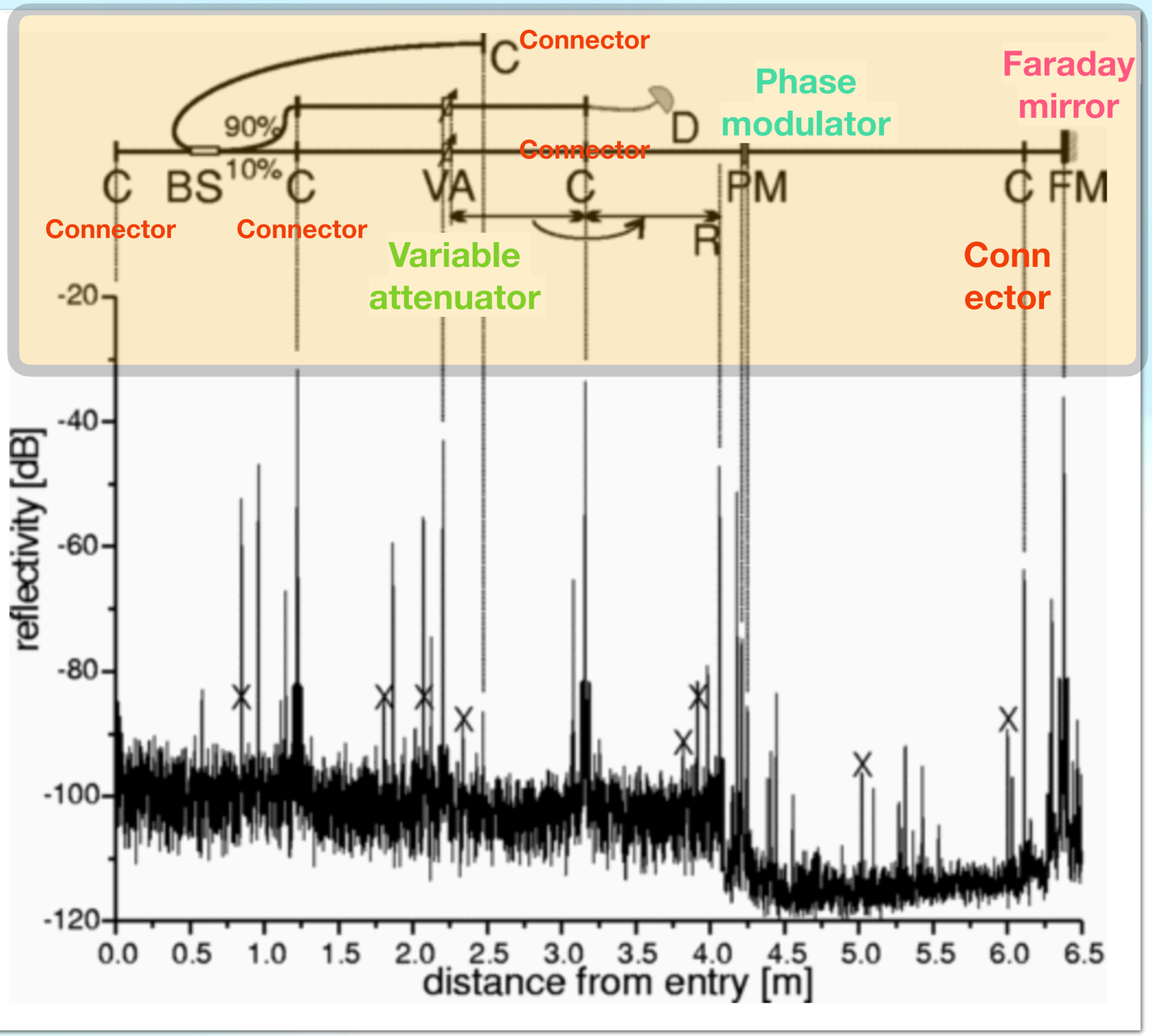
Consequence: a FM automatically compensates any birefringence effect in the fiber: the state going out of the fiber is alway orthogonal to the incoming state.

Replacing the ordinary mirrors M1 and M2 by FMs i.e., adding the FRs, thus ensures that the two pulses P1 and P2 have the same polarization, irrespective of birefringence effects in the delay line M1-M2.

Use of an extra FM in M3 enables one to compensate for the polarization dependence of the PM.

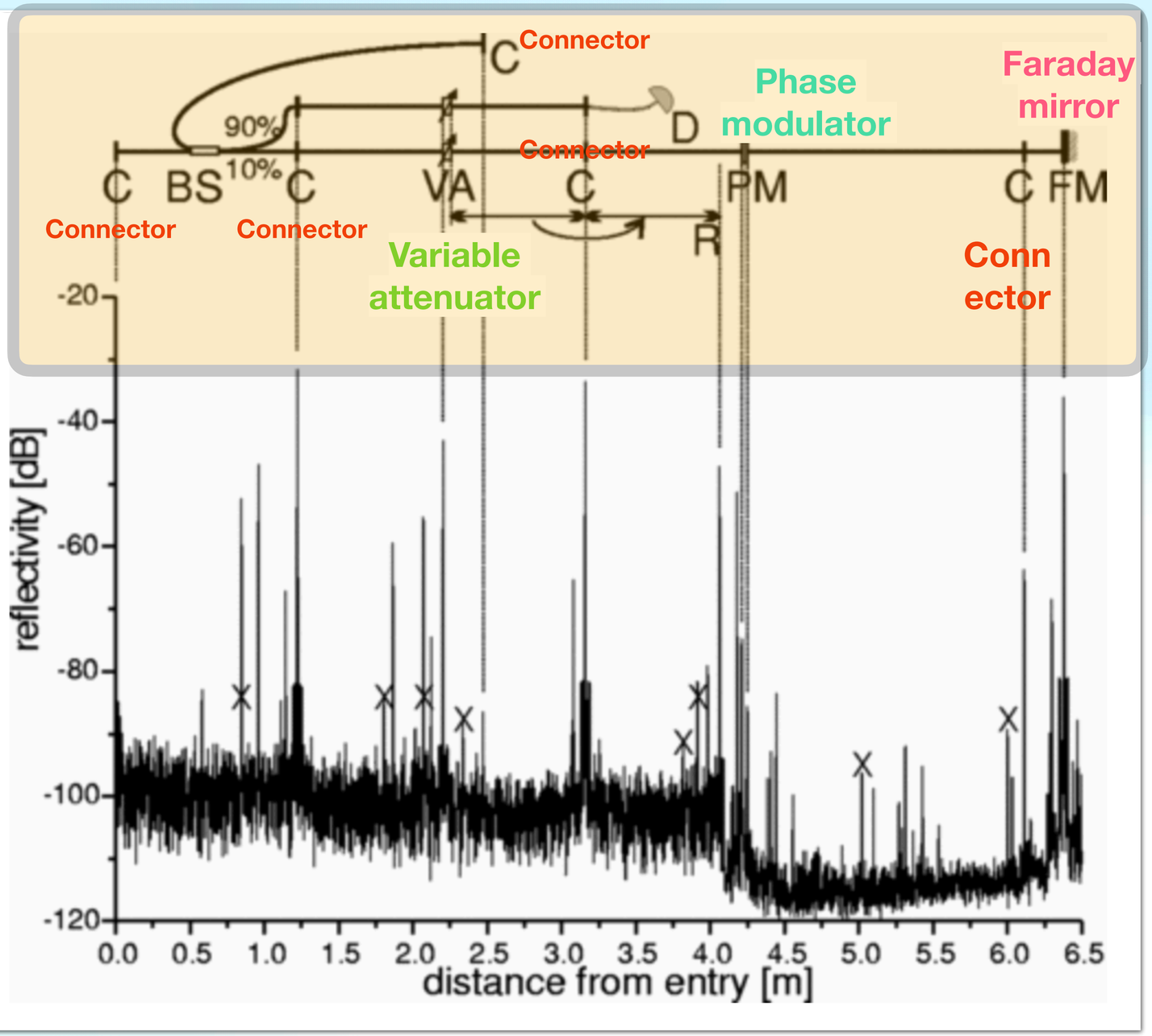


Example of an OFDR trace of Alice's plug-and-play QKD system. **Removed the delay line and set the variable attenuator to its minimal value.**



Example of an OFDR trace of Alice's plug-and-play QKD system. **Removed the delay line and set the variable attenuator to its minimal value.**

A sketch of the optical circuit (at the top) with the corresponding reflections peaks (below).

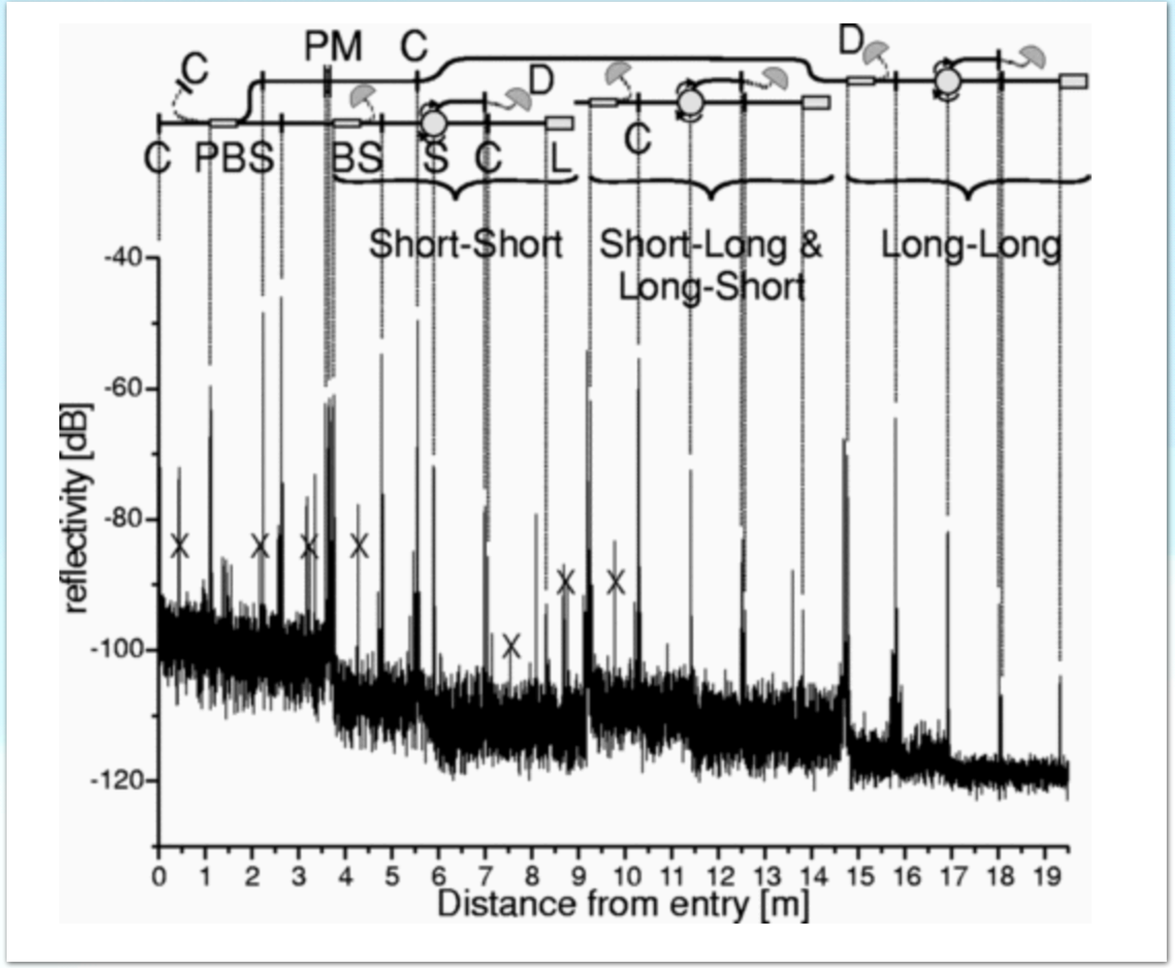


Example of an OFDR trace of Alice's plug-and-play QKD system. Removed the delay line and set the variable attenuator to its minimal value.

A sketch of the optical circuit is displayed at the top with the corresponding reflections peaks below.

Peak "R": corresponds to an example of multiple internal reflections.

Peaks marked with a cross: correspond to spurious reflections between the OFDR and Alice's components.



circulators (S),
polarization beam splitter (PBS),
laser (L).

Example of an OFDR trace of Bob's Plug-&-Play QKD system.

with the additional complication that each peak appears 3 times, because the incoming and reflected light both split in two, following the short and long path of the interferometer. For instance, one can notice that the long arm of the interferometer is about 11.5 meters longer than the short arm.

Fig. \ref{AliceOFDR} and \ref{BobOFDR} present the backscattered light from Alice and Bob's apparatuses, respectively, in the case of our Plug-\&-Play quantum cryptography system\cite{MuGi97,RiGa98}.

They illustrate that indeed quite a lot of information can be gained by probing the apparatuses from the outside.

Let us emphasize that the same is true for all other fiber-based apparatus, like for instance optical amplifiers\cite{OFRDampli} and any other quantum cryptography system.

The details are given in the figure captions.

Note that for the purpose of this demonstration, we removed the about 10 km long delay line in Alice's apparatus, because our laser (contrary to that of Eve) has a coherence length limited to about 1 km).

Note that it isn't yet clear how Eve could probe the setting of the phase-modulator. However, Eve can indeed probe this setting by exploiting the change in birefringence in Titan-indiffused LiNbO3 integrated waveguides, as illustrated in Fig. \ref{PM}. For different kinds of phase modulators, or polarization modulators, it is highly likely that a similar technique applies. Figure \ref{PM} shows that it is easy to distinguish between two phase settings of Alice's phase modulator. To obtain Fig. \ref{PM} we had to keep the phase setting constant during about one second, that is, a much longer time than in the usual use of the crypto system. We also had to adjust the polarization of the probe light and to use a polarization dependant OFDR settings, to maximize the effect. Nevertheless, this result underlines that Trojan horse attacks have to be analyzed seriously.

```
\begin{figure}[htbp]
%\begin{center}
  % Requires \usepackage{graphicx}
  \includegraphics[width=\columnwidth]{figPM.eps}
  \caption{OFDR traces of an integrated optics phase modulator.
  Two different phase settings give raise to clearly distinguishable
  back-scatterings on the output face of the modulator. The two phase settings and the polarization of the probe light are chosen especially to exhibit a very clear effect. The measurement time is of about one second.}\label{PM}
%\end{center}
\end{figure}
```

\section{Hardware counter measures}\label{hardware}
%==
The previous section demonstrated that Trojan horse attacks on badly designed system can be performed using today's techniques. Consequently, every proper implementation should take care that:
\begin{enumerate}
\item the "door" lets in only wavelengths close to the operating wavelength. Any other probe should be eliminated by properly designed filters, and
\item the "door" should be open only during a time as short as possible: the phase modulator, or polarization modulator, or whatever coding device is used, should be activated only during the short time when the legitimate signal is there.
\end{enumerate}

But even these two measures can't completely prevent Trojan horse attacks. Indeed, Eve can multiplex her probe signal with the legitimate signal either in polarization (if time-bin qubits are used by Alice and Bob) or in wavelengths (Eve could reduce the loss of the Q channel, filter out a part of the legitimate signal and use this bandwidth for her Trojan horse attack, see fig. \ref{TH}). Also, in practice, timing has a finite accuracy, hence Eve can add her probes immediately before or after the legitimate pulses.

Consequently, a first conclusion is that every sensitive apparatus (Alice for sure, Bob depending on the protocol) must have an {\bf active control on the intensity of the incoming light}: they should use an auxiliary detector and monitor any incoming light. The software should be designed such as to stop QKD as soon as anormal intensities are detected (actually, for each qubit, there should be a test!).

A first naive idea to circumvent the need for an auxiliary detector is the use of attenuators and/or isolators. However, since Eve is not limited by technology, she could merely send in more intense light\footnote{Every physicists knows that there must be some limit, Eve can't pulse a KJ in an ato-second pulse. At some point, a too large energy concentration should cause the devices to explode, melt or particle pair production starts some nuclear reaction! But this is hard to quantify. Admittedly, the larger the attenuator, the better.}.

A second idea could be the use of an ”optical fuse”, i.e. a device that cuts the quantum channel if a to intense beam passes through it. This is a delicate technological problem. Indeed, there is no such fuse operating for ultra- short pulses. Hence, this does not seem like a practical idea, though one should keep it in mind.

In practice there is a natural fluctuation in the legitimate light and real detectors and electronics also contribute to the fluctuation of the monitoring signal. Hence, being conservative, one has to evaluate how much light can go to Eve without being detected and how much information she could extract from it. Then, appropriate privacy amplification should be applied to Alice and Bob's data. The amount of necessary privacy amplification for any bounded probe by Eve is computed in the next section.

\section{Statistics of Eve's probe light}\label{securityProof}
%==
One may question which state of light Eve should use in order to maximize her information gain. However, it is a well known fact that losses tend to turn any state into a state whose photon number statistics is Poissonian. This is illustrated on Fig. \ref{poissvsgauss} for the cases of 10 and 20 dB losses (i.e. transmissions of 0.1 and 0.01, respectively) and mean photon number, after attenuation, $\mu=0.5$. Since all quantum cryptography systems (should) have attenuators and/or isolators attenuating any light used in a Trojan Horse attack even more severely, it is sufficient to consider light with Poissonian statistics.

```
\begin{figure}[htbp]
%\begin{center}
  % Requires \usepackage{graphicx}
  \includegraphics[width=\columnwidth]{poissvsgauss.eps}
  \caption{Comparison of photon-number distribution for poissonian and binomial distribution of the same average value.
  $\mu$: average number of photons; $t$: transmission factor for Eve's probe light, corresponding e.g the the
  attenuation at Alice's input; $n$: number of photon in the Eve's Fock-state probe light.}\label{poissvsgauss}
%\end{center}
\end{figure}
```

Note that this does also imply that Eve can’t signifi- cantly affect the statistics of the photon number emitted by Alice in the Plug-&-Play configuration, even if she replaced the intense coherent pulse send by Bob by a squeezed state. We ellaborate on this is section VII.