Practical aspects in experimental QKD implementations

Marco Avesani

University of Padova & ThinkQuantum srl

Phd Summer school
Quantum Communication & Space

11/09/2024 Lisbon

ThinkQUANTUM

Università degli Studi di Padova

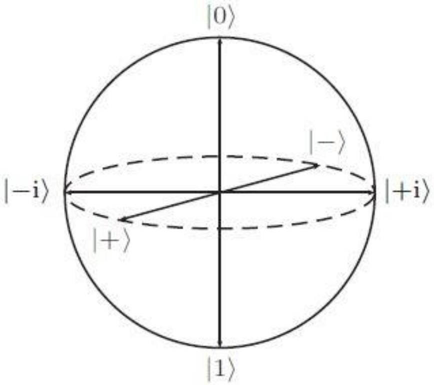
marco.avesani@unipd.it

Time-bin transmitters

BB84 and time-bin/phase modulation

There are several ways to **implement** the **qubits** in a **photonic** system.

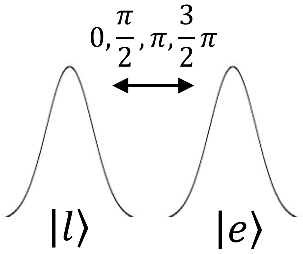
Polarization



Key basis $|0\rangle = |H\rangle, |1\rangle = |V\rangle$

Check basis $|\pm\rangle = \frac{1}{\sqrt{2}}(\,|H\rangle \pm |V\rangle)$,

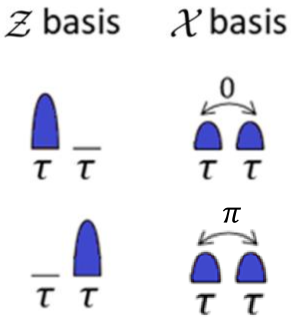
Phase-encoding



Key basis: $|0\rangle = \frac{1}{2}(|e\rangle + |l\rangle)$, $|1\rangle = \frac{1}{2}(|e\rangle - |l\rangle)$

Check basis: $|+\rangle = \frac{1}{2}(|e\rangle + i|l\rangle)$, $|-\rangle = \frac{1}{2}(|e\rangle - i|l\rangle)$

Time-bin encoding

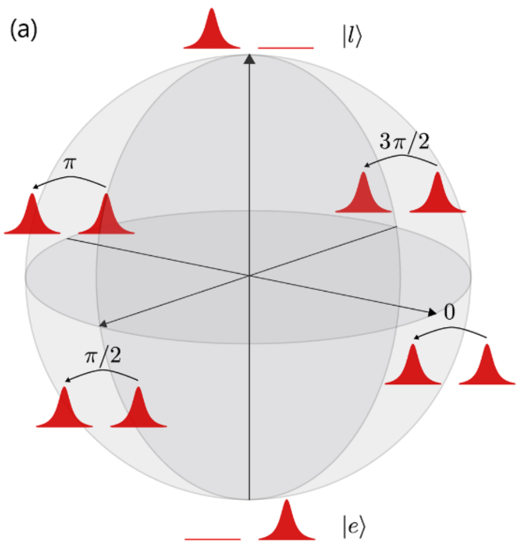


Key basis: $|0\rangle = |e\rangle, |1\rangle = |l\rangle$

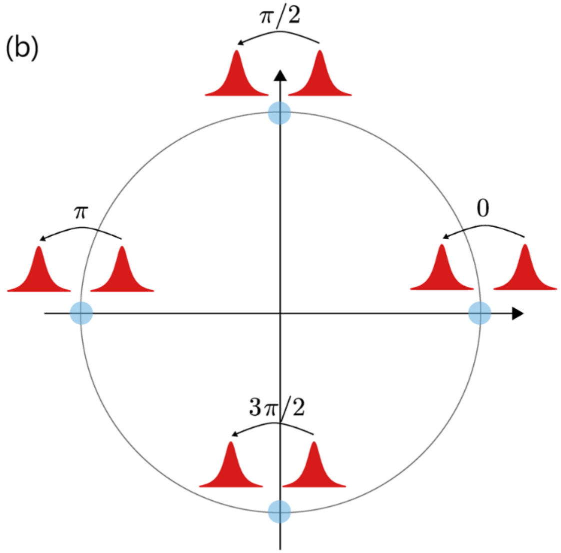
Check basis: $|+\rangle = \frac{1}{2}(|e\rangle + |l\rangle)$, $|-\rangle = \frac{1}{2}(|e\rangle - |l\rangle)$

BB84 and time-bin/phase modulation

Another way to look at the phase or time-bin encoding on the Bloch sphere



Time-bin



Phase encoding

PRO:

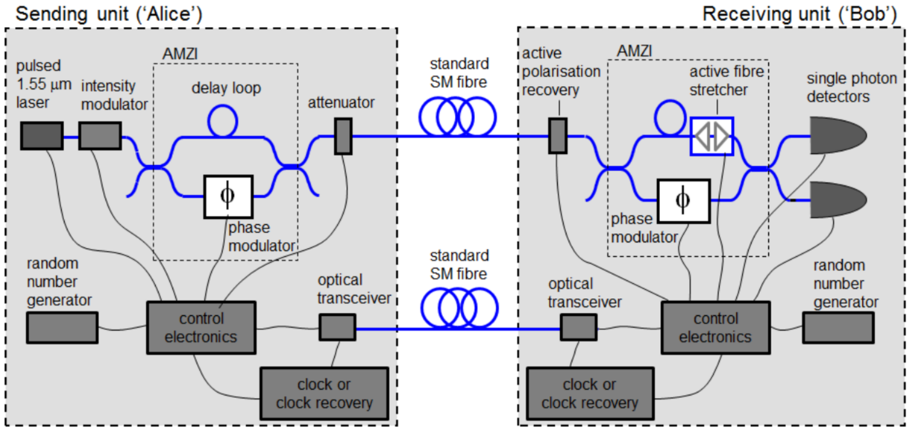
- Insensitive to polarization change of fibers
- Easy to implement with fast all-fiber components

CON:

- Effective half-repetition rate due to time delay between time-bin
- Hard to get low QBER due to stabilization of interferometers
- Harder to realize in free-space

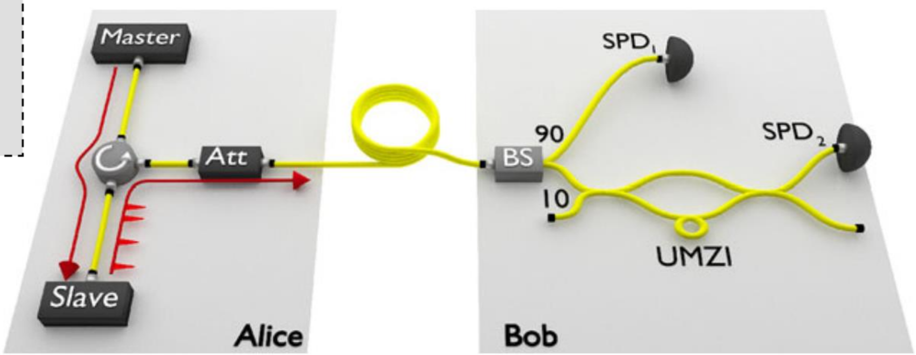
Implementation of time-bin/phase BB84

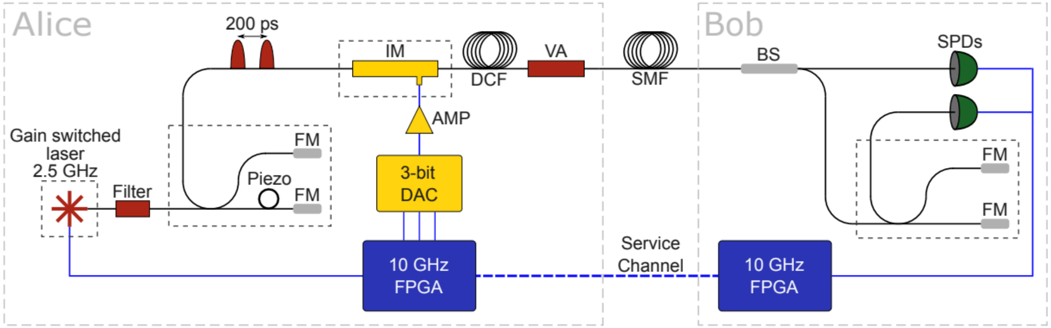
There are several ways to implement the QKD protocol exploiting temporal DOF



Phase encoding

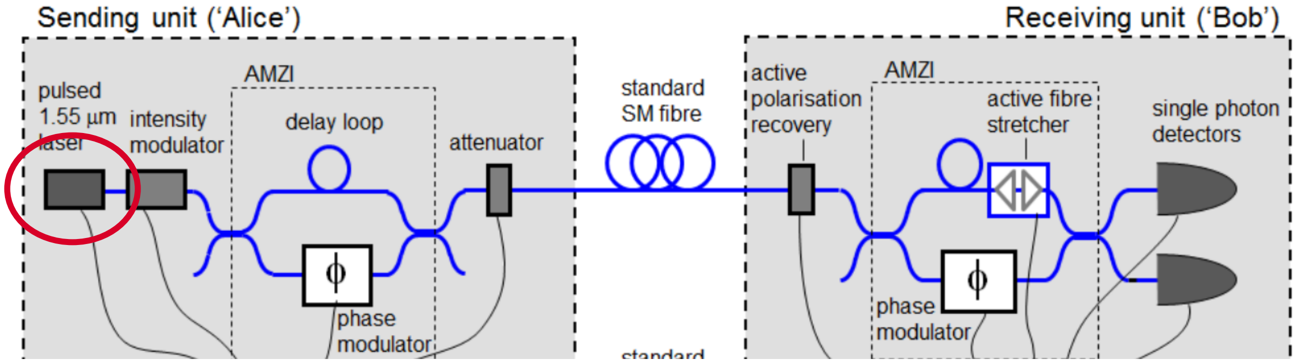
Time-bin encoding (modulator free)





Time-bin encoding

Different components: the Laser



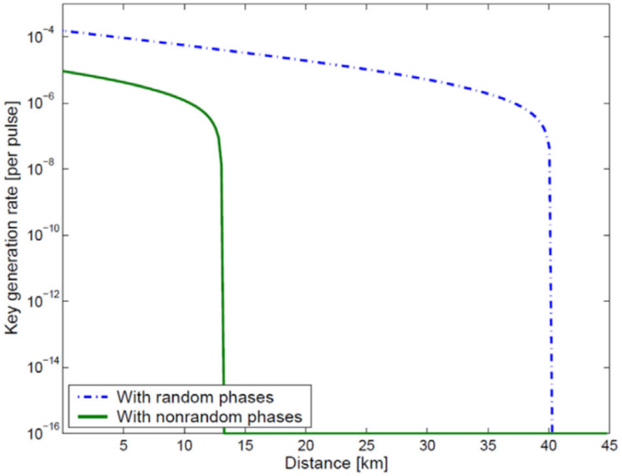
It is **hard** to **generate true single photons**, so **WCP** with **decoy** states are used to avoid PNS attack

However, the decoy analysis assume that the WCP have all uniform and random phases. But coherent states have such distribution:

$$|\alpha\rangle = e^{-\mu/2}\sum_{n=0}^{\infty}\frac{\left(\sqrt{\mu}e^{i\theta}\right)^{n}}{\sqrt{n!}}|n\rangle$$

Instead for uniform phase-randomized WCP:

$$\rho_{\mu} = \int_{0}^{2\pi}\frac{d\theta}{2\pi}|\alpha\rangle\langle\alpha| = e^{-\mu}\sum_{n=0}^{\infty}\frac{\mu^{n}}{n!}|n\rangle\langle n|$$



Huge impact on the SKR!

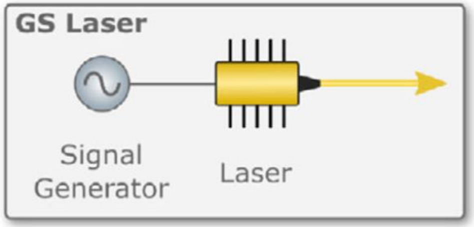
H.-K. Lo, J. Preskill,Quant. Inf. Comput.2007,8, 431.

Different components: the Laser

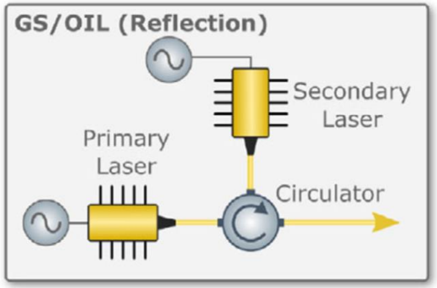
Let's recall the properties that we want for our laser pulses in a QKD setup:

1. **Short optical pulses** (the shorter the pulse the shorter the temporal filter, the higher is the **SNR**. Too short can be challenging for interference)
2. **No chirp** in the pulse
3. **Narrow** spectral **linewidth** (we can use narrower filters to increase the SNR)
4. **Identical power** output between rounds (no correlations between rounds)
5. **Low** temporal **jitter** in the emission
6. **No phase correlations**

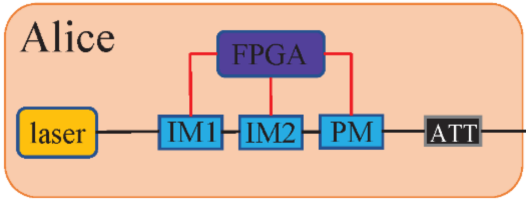
Several ways to generate the PR-WCP, each with pro and cons:



Gain-switch



Optical Injection Locking

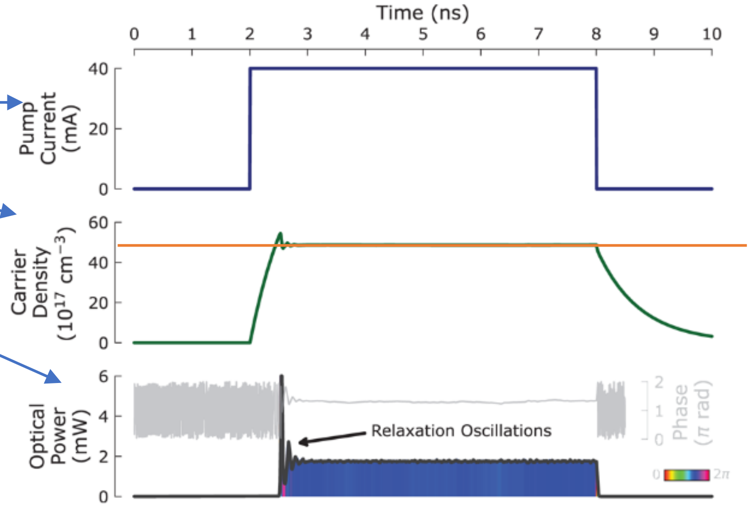


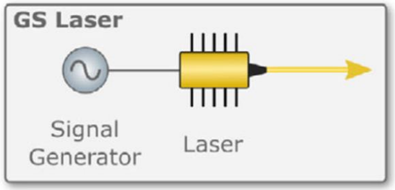
Active phase rand

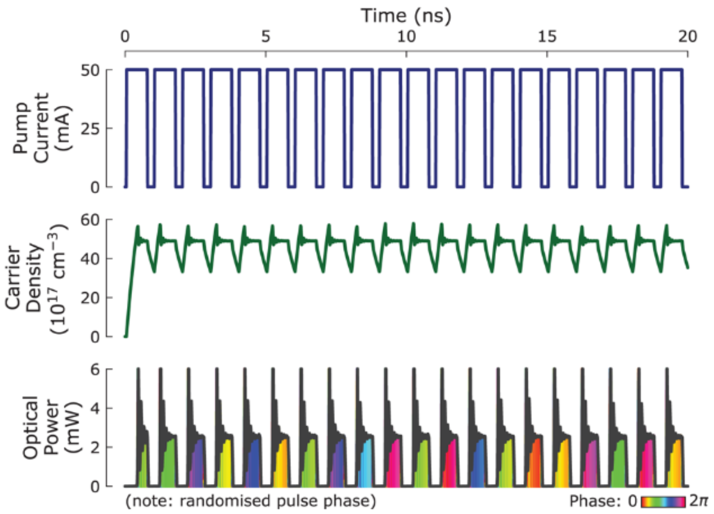
Gain switching:

A simple and effective method is gain-switching:

1. Send short RF signals to the Lasers
2. Carrier density raises until lasing is obtained
3. Fast overshoot, can be used to generate very short pulses (10ps), then relaxation oscillations, and steady-state
4. If enough time to dump the cavity from photons, subsequent pulses have random phases (only vac in cavity)







Technical caveats:

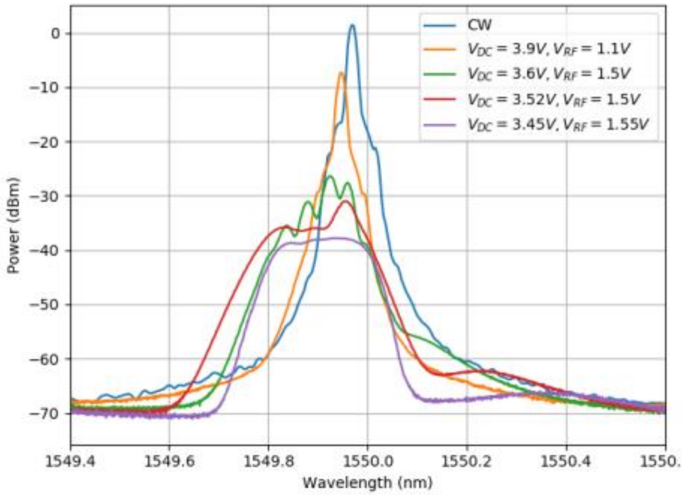
1. Sometimes the amplitude of the RF signal is not sufficient for lasing. Need to add bias. Shift of first curve
2. If bias or frequency too high can destroy phase randomization
3. Non-periodic driving can add intensity correlations

Gain switching:

The approach has several pros and cons:

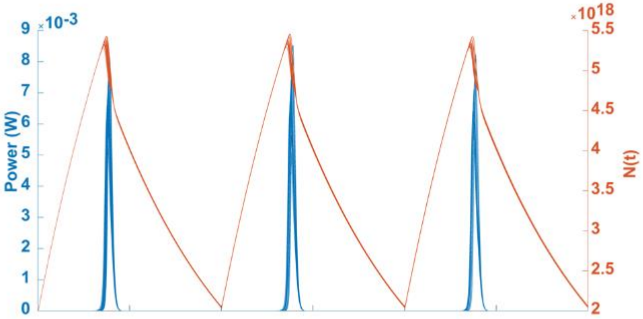
PRO:

1. Simple experimental setup. Just 1 laser and driving electronics
2. Very short optical pulses if only GS part is taken
3. Uniform phase randomization can be achieved
4. High repetition-rate: >5GHz



CON:

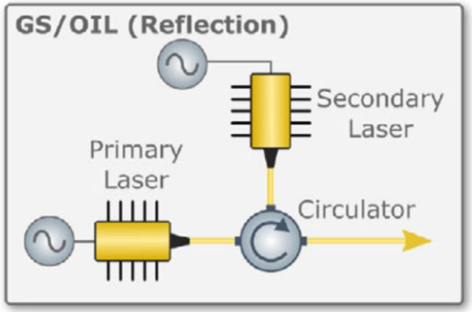
1. Driving of the laser at high speed can be challenging
2. Spectral broadening of the GS
3. Gain-switched pulse is chirped
4. If repetition rate > carrier decay, no or partial phase randomization
5. Carrier fluctuations induce time-jitter in temporal output

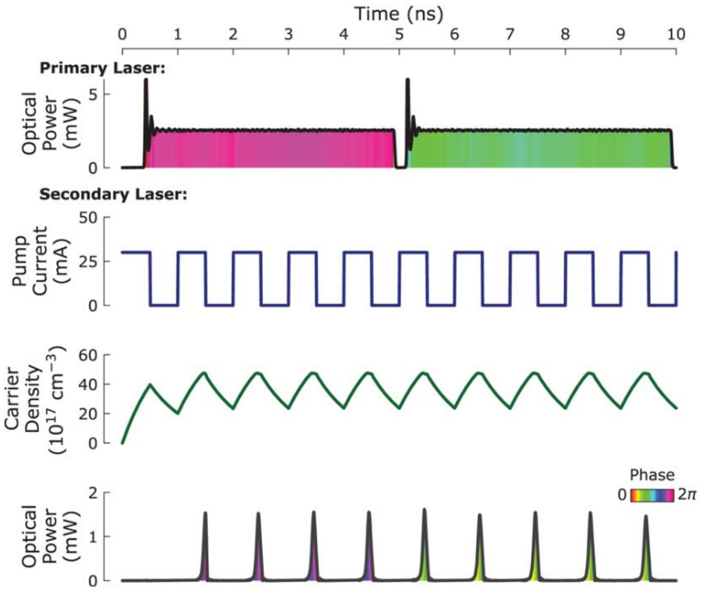


Optical injection locking

Another approach exploits OIL to mitigate some of the problems of GS

1. Two lasers: a master and a slave laser
2. The master laser is GS with long electrical (and so also optical) pulses to get phase randomization
3. The light is injected in the slave laser with a wavelength resonant with the cavity of the slave
4. The slave laser is GS with seed light from the master in the cavity a with short pump
5. A circulator is used to get the reflected light out





When the slave laser is Gain-Switched the stimulated emission is seeded by the light from the master laser and the slave pulse “inherits” the phase of the master laser

Optical injection locking

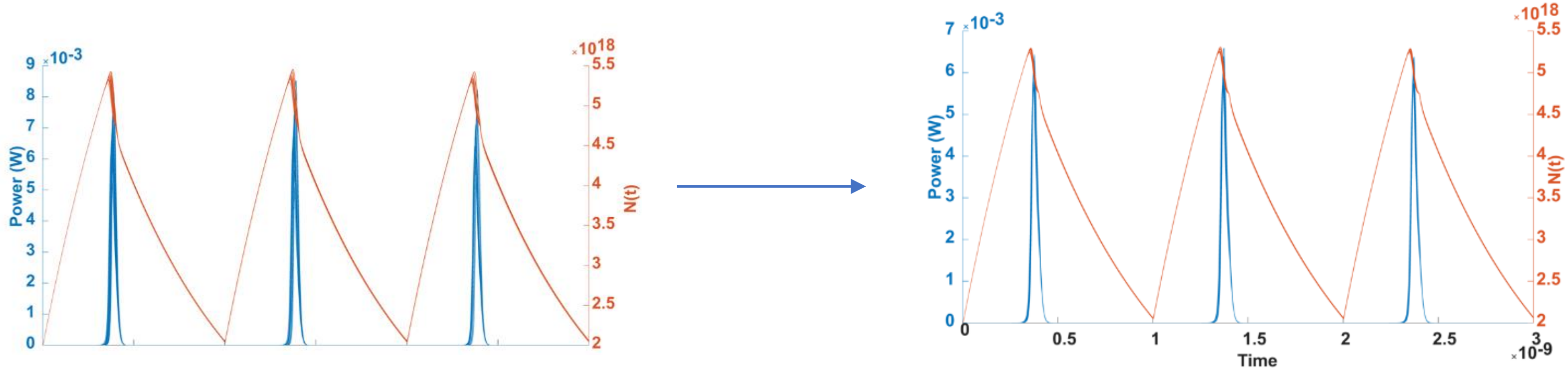
The approach has several pros and cons:

PRO:

1. Reduced linewidth broadening thanks to seeding
2. Reduced temporal jitter of the output pulse
3. Increased relaxation oscillation frequency, more stable pulses
4. More stable power output

CON:

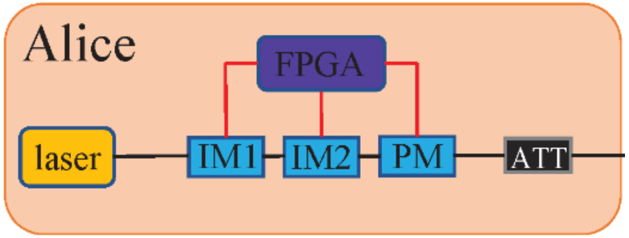
1. More complex and expensive solution
2. Requires tuning and lock of the wavelength of the two lasers (can be challenging in case of very narrow lasers)
3. Have to control the optical power injected
4. More sensible to temperature fluctuations



Active phase randomization

Finally, the last method is to use an active modulation

1. A CW laser is operated in continuous mode
2. One or more Intensity modulators are used to chop the CW light into pulses
3. An inline phase modulator is used to add random phases to each pulse



PRO:

1. Smallest linewidth (can get to Fourier limit)
2. Only one laser

CON:

1. Requires more modulators
2. Requires active choice and randomness
3. Need to stabilize the phase and IM modulators
4. Can be correlations due to finite-bandwidth
5. Can be fluctuations due to temperature or electrical pulse imprecision

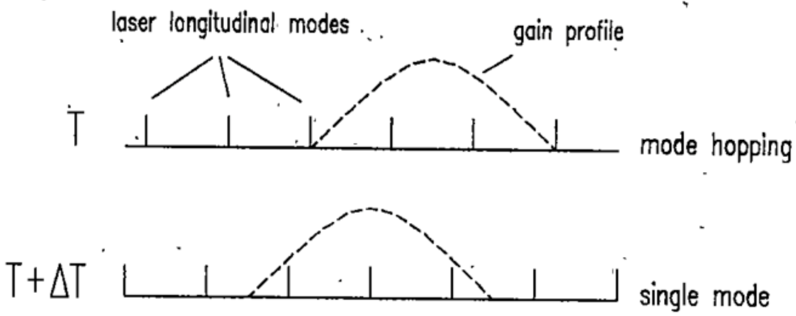
Other important facts about the lasers

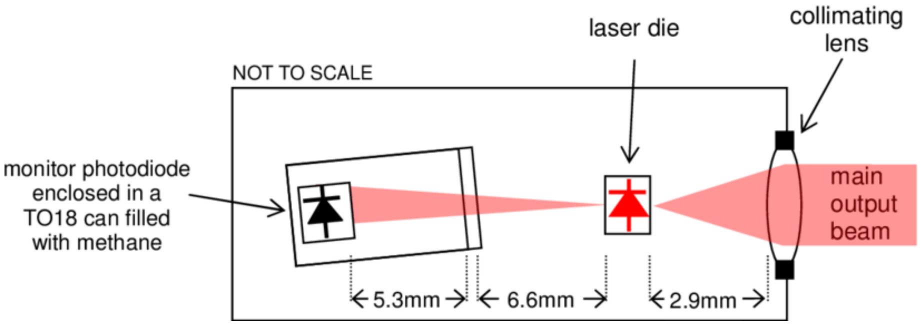
When operating a laser in a QKD system the re are other important effect to keep in mind:

- **Temperature and current tuning:** by changing the temperature of a laser, the cavity is changed and so also the wavelength. Typical values for 1550nm lasers I 0,1nm/cm. Similarly increasing the current also shifts the wavelength. Temperature usually stabilized with TEC. This is necessary at high power to dissipate heat.

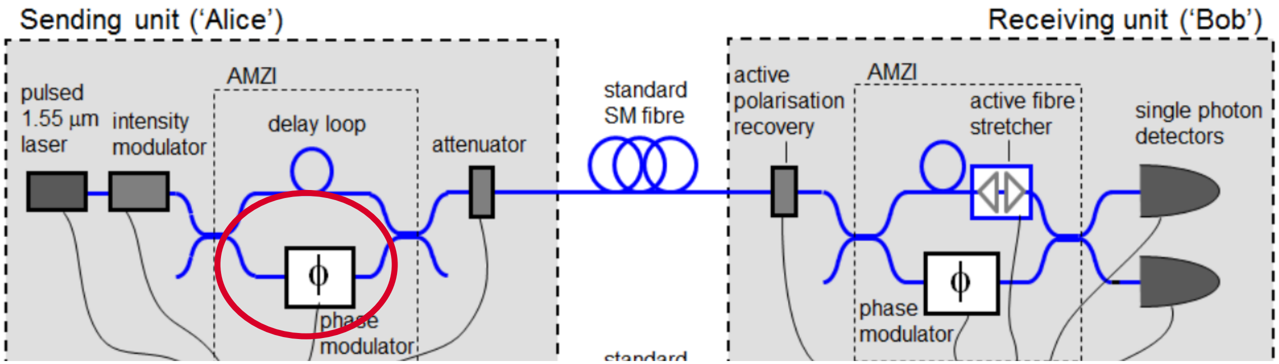
- **Mode hopping:** if the gain profile of the laser matches two competing modes of the cavity with almost the same gain, the laser can start “hopping” between the two modes. This can increase power fluctuations and induce beatings

- **Aging:** with time the power of semiconductor lasers is reduced. Usually on DFB a photodiode is included for compensation





Phase modulator

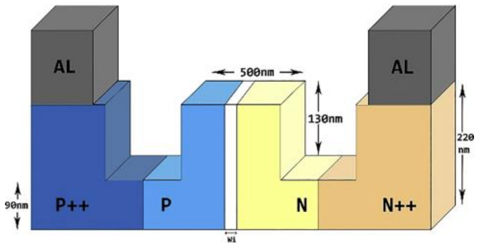


A fundamental component for almost every QKD setup is the phase modulator

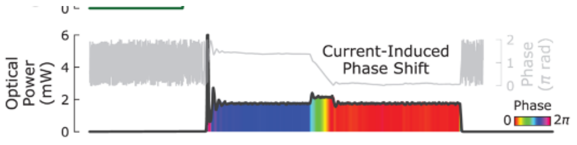
As the name says, it allows to change the phase of the light passing through. We will analyze two ways to modulate the phase

Several approaches: we will analyze

Lithium-niobate phase modulators



Carrier injection/depletion modulators

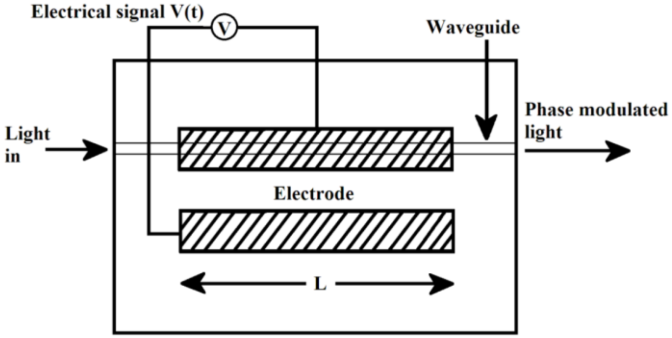


Direct laser modulation

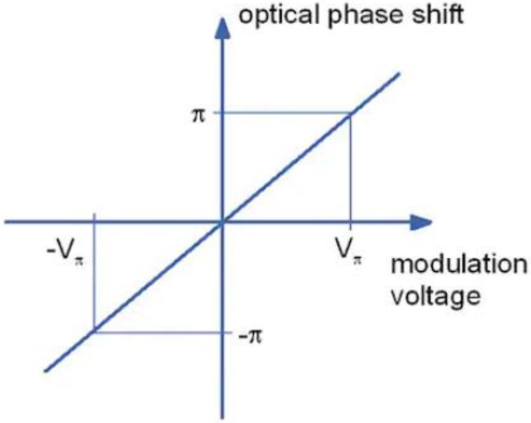
Electro-optic Phase modulator

The electro-optic phase modulator is a device based on a nonlinear optical material that has a large χ^2 coefficient. Typical materials are LiNBo3, ppKTP.
For such materials we have the Pockels effect, where the refractive index depends on the applied electric field

$$n(E) \approx n + \underbrace{\frac{2}{\epsilon_0 n}\chi^2 E}_{\Delta n(E)}$$



For a beam of light travelling in the waveguide the difference in refractive index implies a difference in the time for the propagation of the light, which is a difference in the phase.



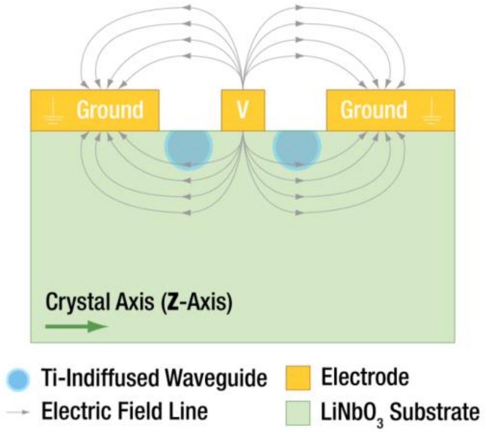
$$\Delta t(E) = \frac{\Delta n(E)\, L}{c}$$

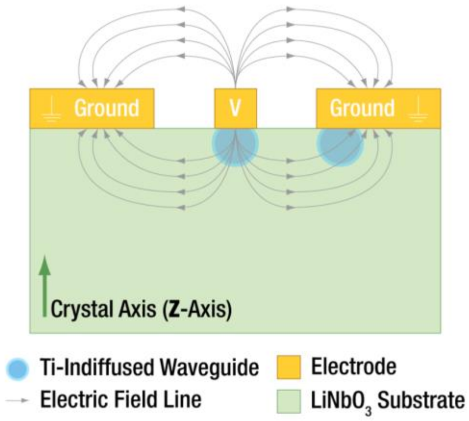
$$\Delta\phi(E) = \omega\, \Delta\text{t}(\text{E})$$

Linear around the 0

Working with phase modulators

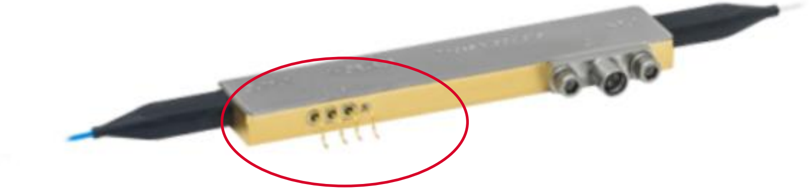
Polarization support: fiber LN phase modulator come in two types: Z-cut or X-cut. The name refers to the orientation of the waveguides with respect to the crystal axis.
X-cut: have symmetric electrodes, higher Vpi, no chirp and support only one polarization
Z-cut: have asymmetric electrodes, lower Vpi, chirp and support both polarizations with different modulation efficiencies





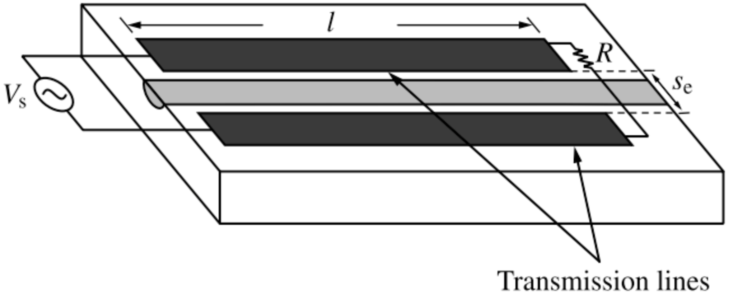
For a light that is $\frac{1}{\sqrt{2}}(|\mathrm{H}\rangle + |V\rangle)$, for a modulation with V we get $\frac{1}{\sqrt{2}}\left(\mathrm{e}^{i\Delta\phi_o(V)}\,|\mathrm{H}\rangle + \mathrm{e}^{i\Delta\phi_e(V)}|V\rangle\right)$

Stability: the refractive index in the LN does not only depend on external electric fields but also by temperature, and mechanical stresses and input RF power. Fiber phase modulators usually add an additional $\Delta\phi(t)$ due to these effects. They require external feedback loop to stabilize.



Driving phase modulators

Travelling wave modulators: the electrodes placed on high-speed phase modulators are made of strip transmission lines. The RF modulation signal is injected at one end, propagates along the same direction as the optical wave, and terminates at the end on a 50 ohm termination.



Two **limits** on bandwidth:

- **Speed mismatch between RF and optical signal**
- **Microwave attenuation at high frequencies**

Beware, if used in reverse mode the modulation efficiency is lower due to the reduced interaction between the travelling RF signal and the optical signal.

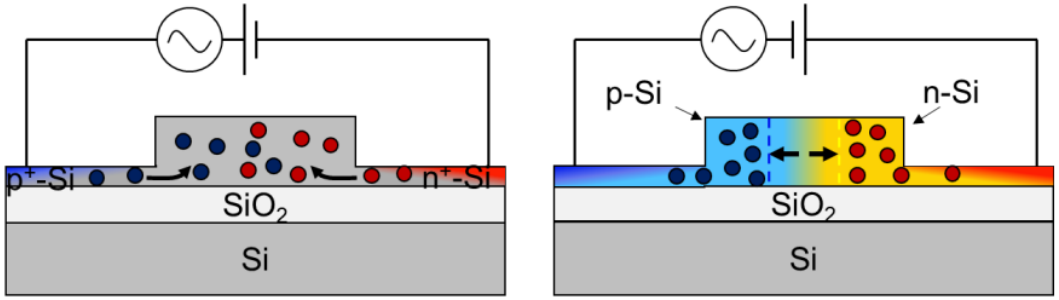
Driving the pm: driving the phase modulator at high speed can be challenging. The electrodes are mainly a capacitive load with few pf of capactitance. However, the 50ohm termination in travelling wave requires to supply a significat amount of current.

Typical Vpi are between 4 to 8V, and the 50ohm load usually requires to use power broadband amplifiers.

Carrier injection/depletion phase modulators

They are mostly used in silicon-based devices, where it is hard to integrate different materials due to the fabrication process.

Due to the plasma dispersion effect, the density of free carriers in a semiconductor, changes both the real and imaginary parts of the refractive index.



$$\Delta n = \frac{-e^2\lambda_0^2}{8\pi^2 c^2 \varepsilon_0 n}\left(\frac{\Delta N_e}{m_{ce}^*} + \frac{\Delta N_h}{m_{ch}^*}\right)$$

Where $\Delta N_{e,h}$ is the variation of number of electrons and holes

By doping with both p and n dopants the region across a waveguide we can add an high density of carries close to the waveguide while creating a p-n junction. By applying an electical field we can remove (or add) carriers to the junction, changing the refractive index.

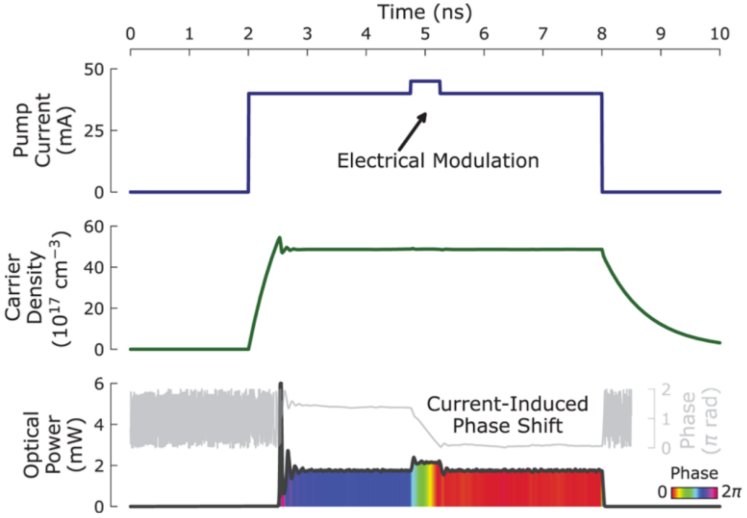
Can be fast (20 GHz +) but unlike LN PM they behave like diodes. Can be driven only in reverse mode otherwise the junction is opened.

Vpi around 1V/mm

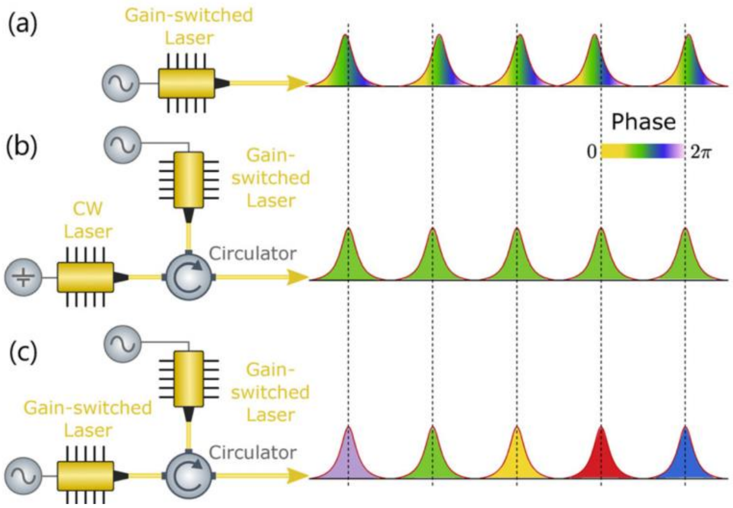
Direct laser phase modulation

Another method to directly modulate the phase of the optical pulses is to exploit the dynamics of the laser. For DFB lasers the carrier density is related to the refractive index of the gain medium.

Changing the current will change the refractive index, changing the effective length of the cavity and thus the wavelength. After the modulation is off the wavelegth is changed back to the original.
However the accumulated phase is retained.



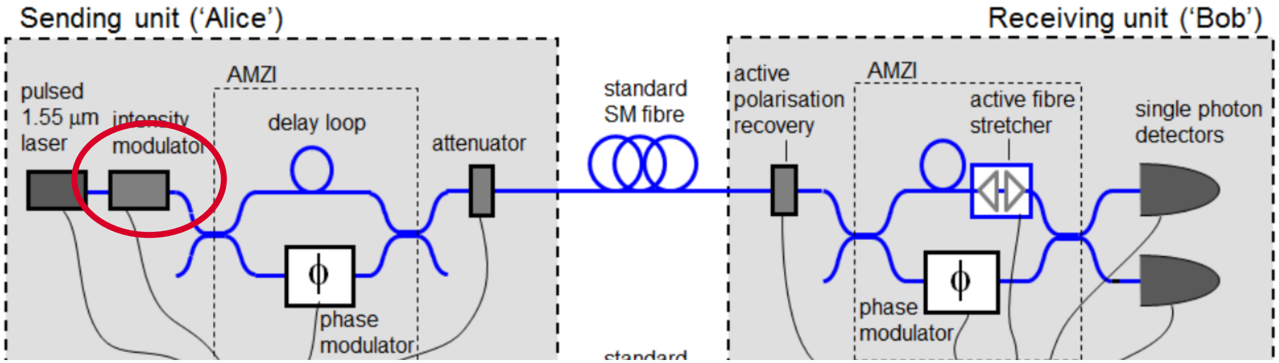
However the change in phase will induce changes in intensity. To avoid this effect the lasers are placed in the master-slave configuration, combining with the global phas randomization.



The modulation can be deterministically performed by changing amplitude and length of the electic mod.

Extremely efficient: for 250ps mod 7,4ma!

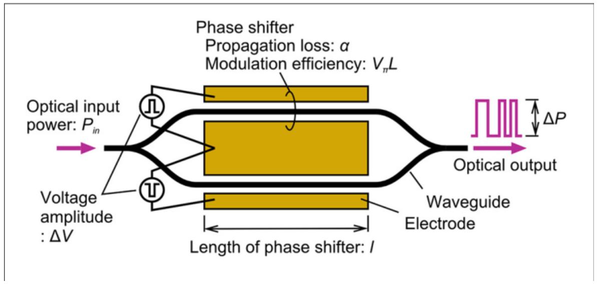
Intensity modulator



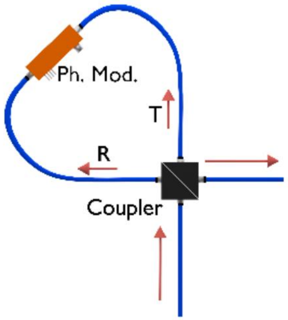
Another important component for a QKD setup is the **Intensity Modulator**

This component is required for the decoy-state method where two or more intensity levels need to be generated.

Several approaches: we will analyze

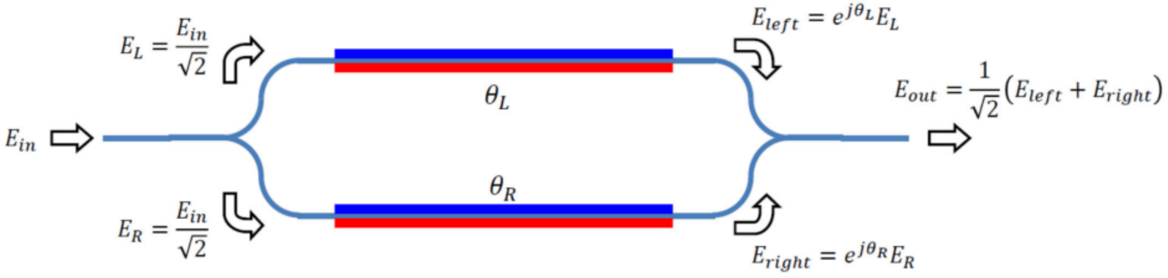


Mach-Zehnder modulator



Sagnac-loop IM

Mach-Zehnder modulator



$E_L = \frac{E_{in}}{\sqrt{2}}$
E_{in}
$E_R = \frac{E_{in}}{\sqrt{2}}$
θ_L
θ_R
$E_{left} = e^{j\theta_L} E_L$
$E_{out} = \frac{1}{\sqrt{2}}(E_{left} + E_{right})$
$E_{right} = e^{j\theta_R} E_R$

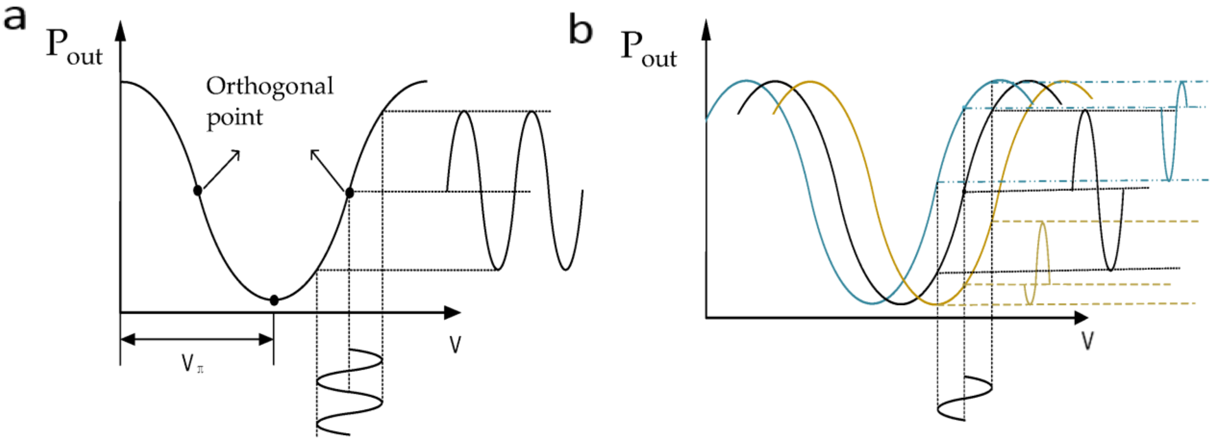
The Mach-Zehnder modulator allows to use the interference effect in a Mach-Zehnder interferometer to modulate the intensity of the output light. In this case a phase modulator in the MZ is used to change the phase of the light

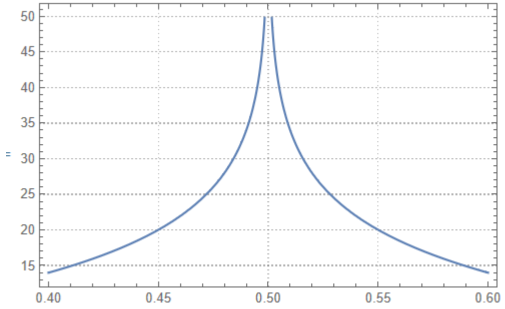
$$I_O = I_i \cos^2\left(\frac{\phi(V)}{2} + \frac{\phi_0(t)}{2}\right) \qquad T(V) = \cos^2\left(\frac{\phi_0}{2} + \frac{\pi}{2}\frac{V}{V_\pi}\right)$$

With push-pull driving, i.e. driving the up and low modulator with differential signals we remove the chirp and reduce by half the the V_π

Typically MZ intensity modulator are produced with X-cut modulators

Disadvantages of Mach-Zehnder modulator





The MZ modulator inherits several disadvantags of the MZ interferomenters and from the phase modulators:

- Very sensible to change in the path of the arms due to temperature
- Very sensible to change in the phase in the arms due to phase modulator drifts
- Fluctuations in the phase change working point… direct change in intensity
- Fluctuations in the phase change working point: change in the ratio
- They usually work on the orthtogonal points: small variation of the electrical signals mean high variations in the intensity output
- Extinction rate depends by the balancing of the BS
- Hard to get over 25/30db of ER

$$ER = -20 \log10(|2R - 1|).$$

A solution with two way configurations

A better solution employs an asymmetric Sagnac interferometer with PM fiber:

- Light is split into clockwise and anticlockwise path
- The phase modulator is placed asymmetrically so that clockwise and counterclockwise pulses can be addressed independently
- By either modulating the CW or the CCW pulse one can add a positive or negative phase shift
- Since both pulses travel in the same optical path, phase shifts experienced by both CW and CCW will be canceled out

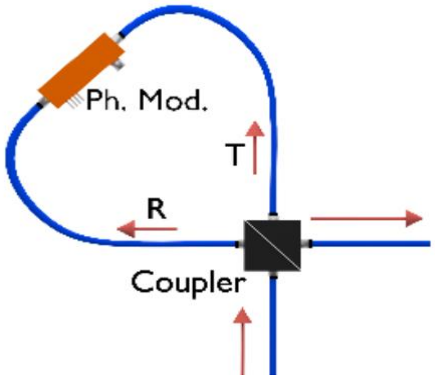
$$I \propto R^2 + T^2 + 2RT\cos(\Delta\phi)$$

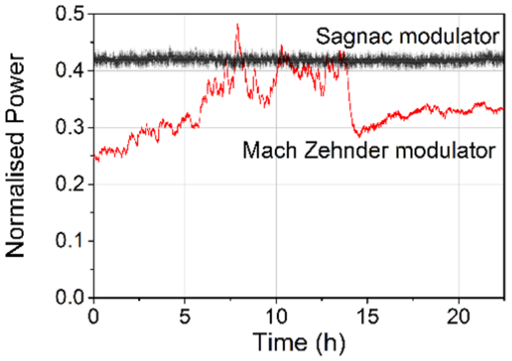
PRO:

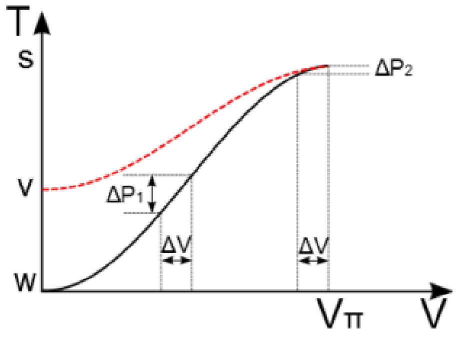
- Higher temporal stability due to cancellation of common phases
- Tunable ratio
- Lower fluctuations if working point adjusted around the max of the transfer function
- Constructive interference with no modulation is useful for pulse chopping

Cons:

- Max frequency due to travelling wave structure



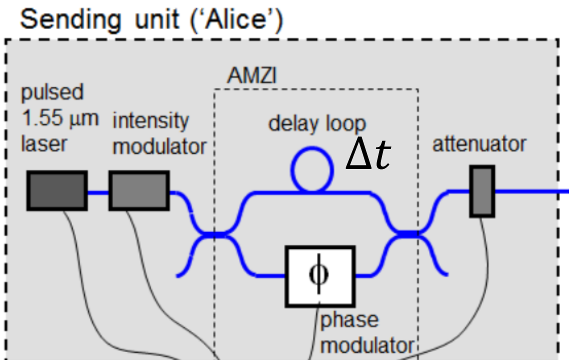




The encoding interferometer

Both for phase and time-bin implementations it is necessary to create the photon's superposition of the two temporal modes that are used to encode the phase.

One of the most common solution is to employ an unbalanced Mach-Zehnder interferometer, where one arm is longer than the other.



In this way the input pulse is mapped into to orthogonal pulses at different times.

$$|i\rangle \rightarrow \cos\left(\frac{\theta}{2}\right)|e(t)\rangle + \sin\left(\frac{\theta}{2}\right)e^{i(\phi(V)+\phi_o)}|l(t+\Delta t)\rangle$$

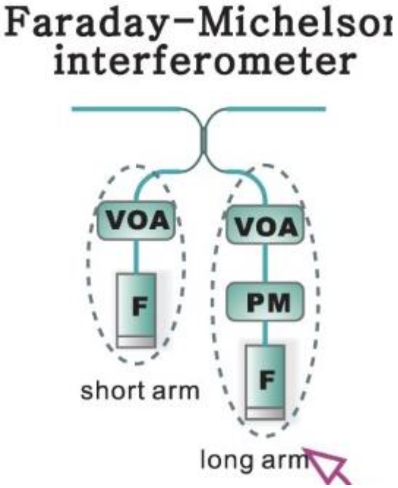
Being based on a MZ interferometer also this solution suffers the same stability problems discussed in the previous cases, which are related to the term ϕ_o.

However, another problem is related ot the **polarization**: the interference occurs only for states with the same polarization. If the polarization of the light at the reconbining BS is different the visibility will be lower.

Relevant for fiber implemetations with SM

The Faraday-Michelson interferometer

Again, to solve instability problems a two-way solution is used



The (unbalanced) Faraday-Michelson interferometer is a Michelson interferometer where the mirrors are replaced with Faraday mirrors.

The Faraday mirror, in the reference frame of the photon, applies a σ_x transformation mapping

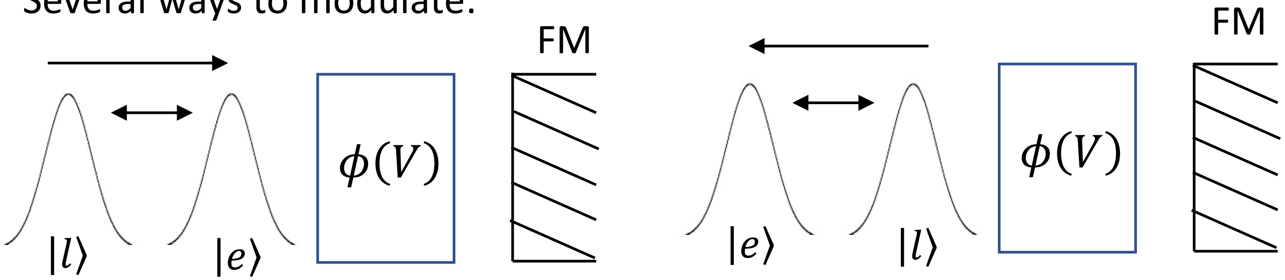
$$|H\rangle \rightarrow |V\rangle, |V\rangle \rightarrow |H\rangle, |D\rangle \rightarrow |D\rangle, |A\rangle \rightarrow |A\rangle, |L\rangle \rightarrow |R\rangle, |R\rangle \rightarrow |L\rangle$$

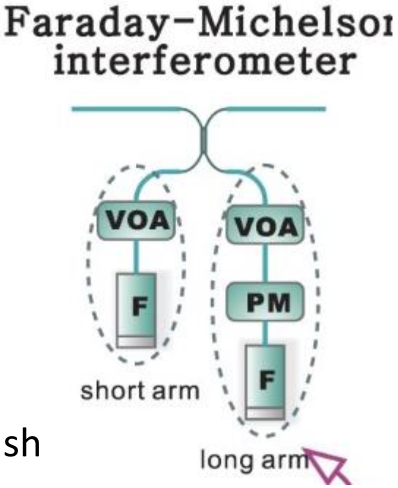
Placing the faraday mirror at the end of the arm, we ensure that any relative phase drift experienced by the light in the forward direction is compensated in the way back

$$|H\rangle + |V\rangle \rightarrow \ |H\rangle + e^{i\phi_0}\ |V\rangle \rightarrow |V\rangle + e^{i\phi_0}\,|H\rangle \rightarrow e^{i\phi_0}|H\rangle + e^{i\phi_0}|V\rangle = |H\rangle + |V\rangle$$

The Faraday-Michelson interferometer

Several ways to modulate:





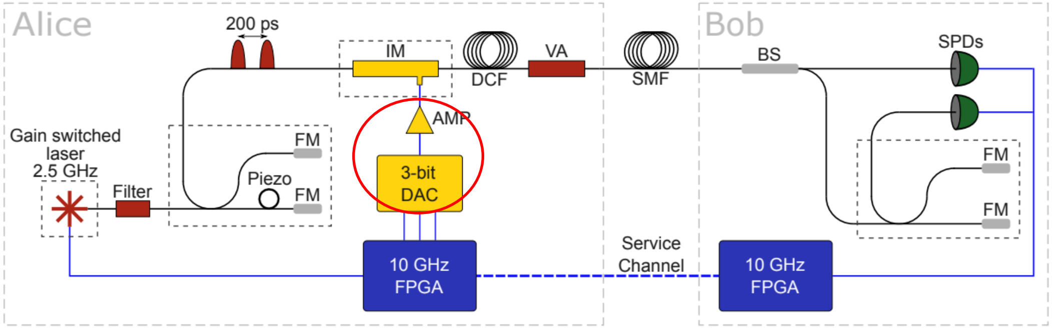
One or both pulses before the FM, one before one after the reflection, or in push pull

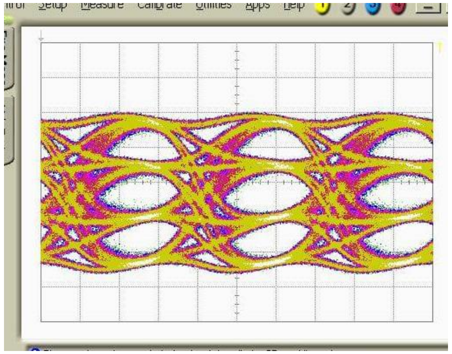
The big advantage is that many of the instabilities are compensated, higher visibilities: typically >98%

However, path difference is doubled due to the reflection. Increased phase fluctuations due to temperature changes

Also additional time requirements on the modulation: the original signal gets back to the phase modulator after $2\Delta \mathrm{l}\frac{\mathrm{n}}{\mathrm{c}}$

Electronic driving

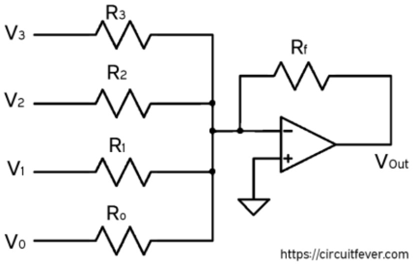




For most of the discussed implementations the timing requirements are quite challenging and jitter or low rise-time of the modulation signals imply an intersimbolic interference between the time-bins or subsequent pulses that increase the QBER.

For example: 200ps of separation requires rise-time of less than 50/70ps, equivalent to bandwidth of around 7GHz.

CMOS cannot provide such high speed, the only standards are ECL or CML with single-ended swings of 400mV into 50ohm load. However, typically IM or PM have Vpi voltages around 4 to 8V. This requires RF amplifier with sufficient BW, gain and saturation power of around 23-25dbm.



https://circuitfever.com

If multi amplitude is required need to add an RF DAC that maps parallel inputs into different amplitudes

Polarization transmitters

Efficient-BB84 and polarization modulation

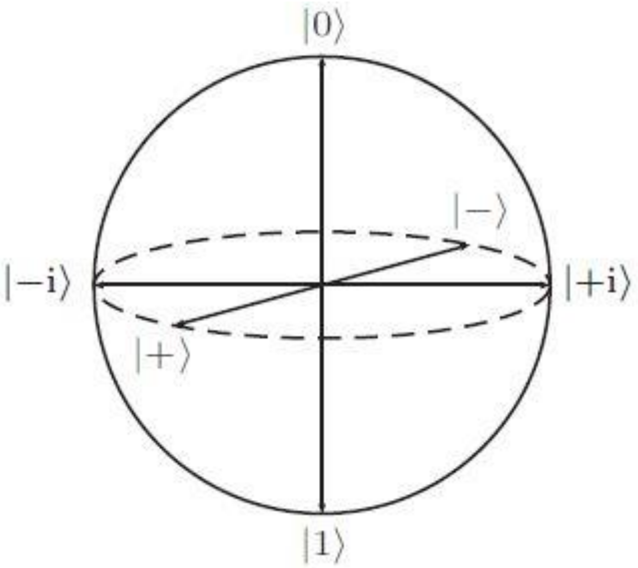
One of the first and simplest implementations of the BB84 protocol were done using the polarization of photons as degree of freedom.

Usually, the computational basis is chosen as the H/V basis:

$$|0\rangle = |H\rangle, |1\rangle = |V\rangle$$

While one of the other two is chosen as check basis:

$$|\pm\rangle = \frac{1}{\sqrt{2}}(\,|H\rangle \pm |V\rangle), |L\rangle, |R\rangle = \frac{1}{\sqrt{2}}(\,|H\rangle \pm i|V\rangle),$$

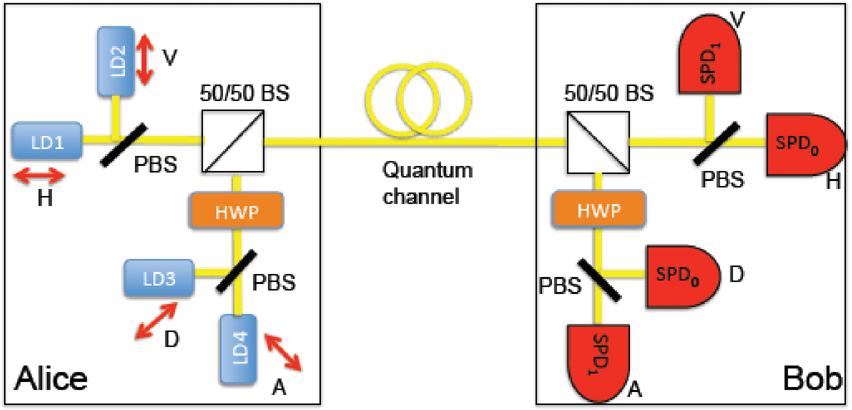


Polarization has several advantages:

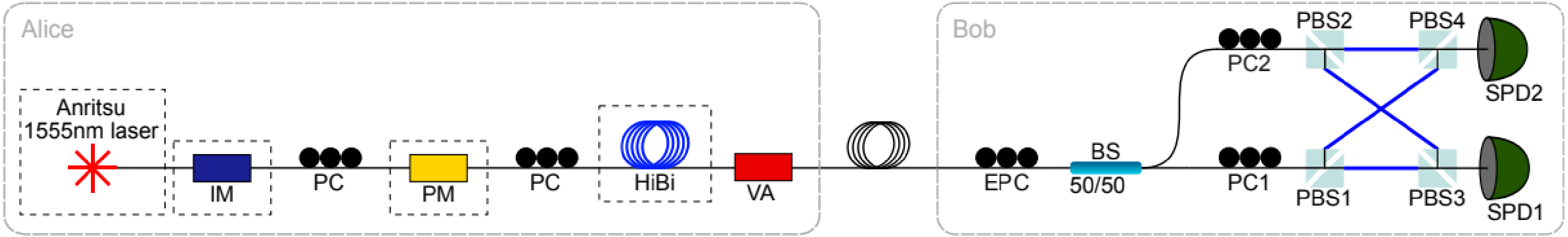
- **Robust for free space transmission**
- **No need of interferometric setup** and can be prepared and measured easlily

Implementation of polarization-based BB84

There are several ways to implement the QKD protocol exploiting the polarization



Four independent lasers
And four SPD

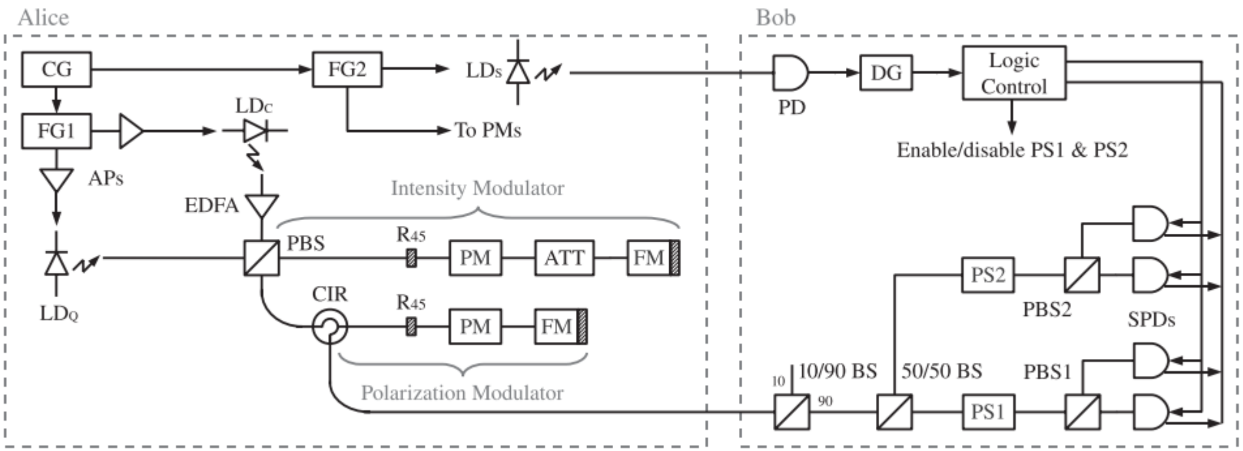


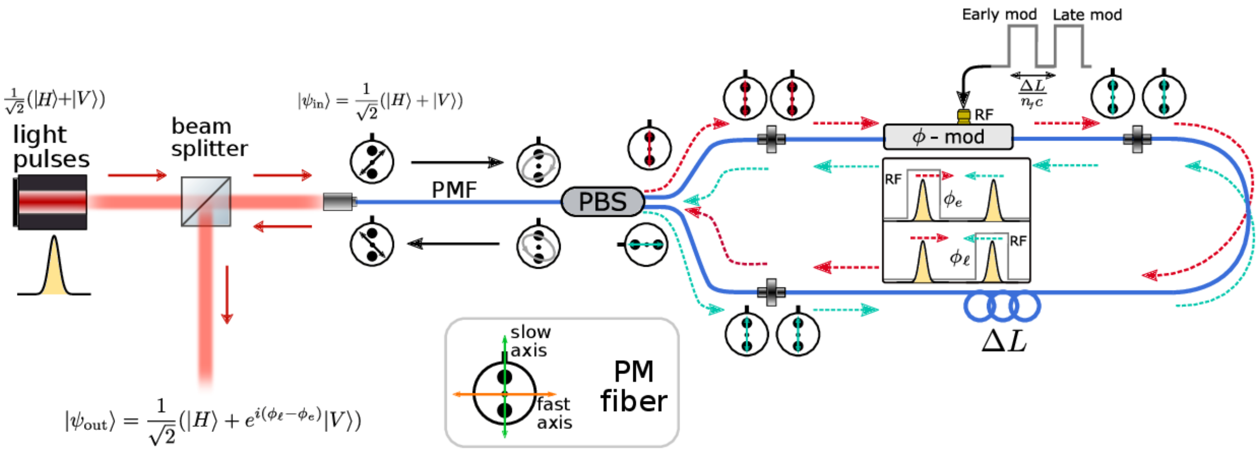
Inline phase modulator @45 deg and polarization multiplexed SPD

Implementation of polarization-based BB84

There are several ways to implement the QKD protocol exploiting the polarization

Phase modulator@45 in two-way configuration with Faraday mirror



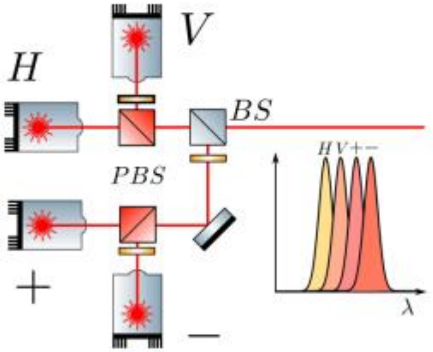


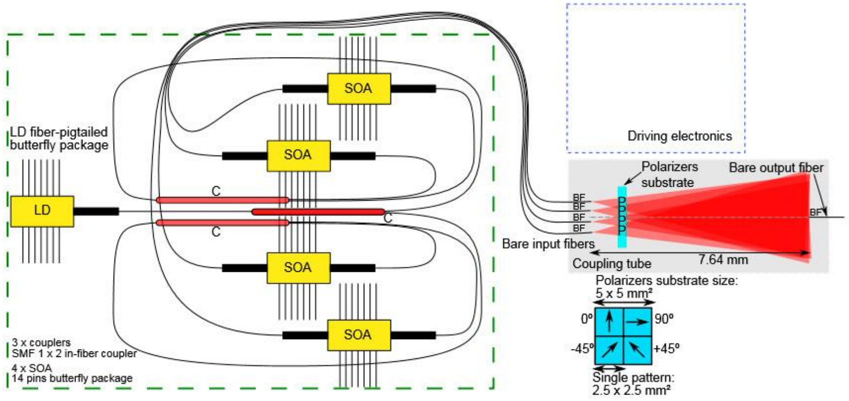
$\frac{1}{\sqrt{2}}(|H\rangle+|V\rangle)$
light pulses
beam splitter
$|\psi_{in}\rangle = \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle)$
PMF
PBS
Early mod
Late mod
$\frac{\Delta L}{n_g c}$
RF
ϕ - mod
RF
ϕ_e
ϕ_ℓ
RF
ΔL
$|\psi_{out}\rangle = \frac{1}{\sqrt{2}}(|H\rangle + e^{i(\phi_\ell - \phi_e)}|V\rangle)$
slow axis
fast axis
PM fiber

Pognac/ Ipognac modulator with Sagnac loop

Independent lasers

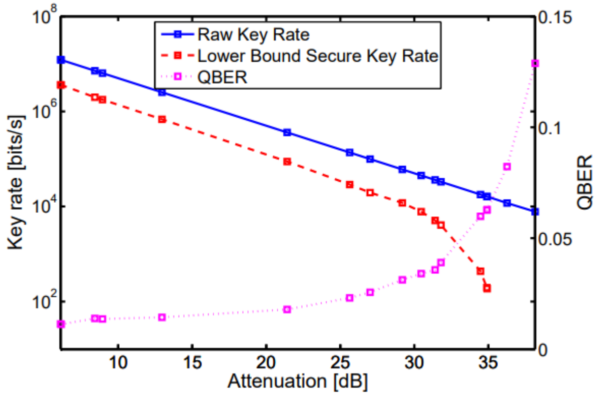
One possible implementation is to use 3 or 4 independent lasers or SOA, together with different polarizing elements and combining them




SOA
SOA
SOA
SOA
LD
C
C
C
LD fiber-pigtailed butterfly package
3 x couplers SMF 1 x 2 in-fiber coupler
4 x SOA 14 pins butterfly package
Driving electronics
Polarizers substrate
Bare output fiber
BF
BF
BF
BF
BF
Bare input fibers
Coupling tube
7.64 mm
Polarizers substrate size: 5 x 5 mm²
0°
90°
-45°
+45°
Single pattern: 2.5 x 2.5 mm²

Each laser is turned on independently selecting the required polarization sate. This simple solution has several drawbacks.

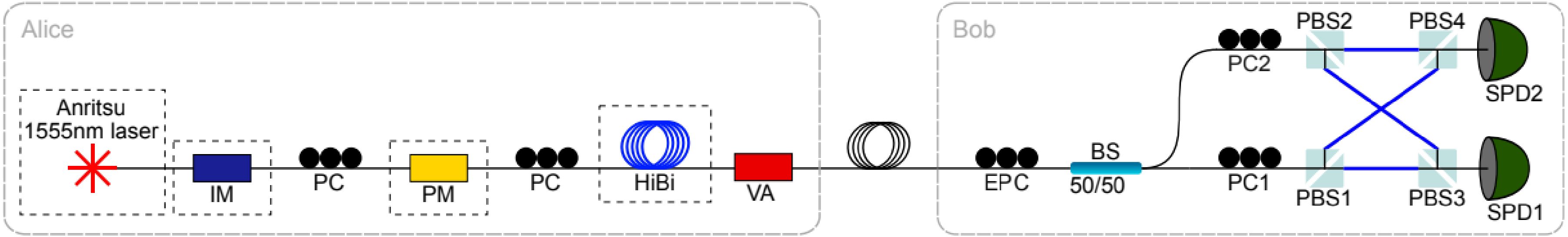
- **Expensive and power hungry** (4 lasers, 4 TEC, 4 driving circuits)
- **Security:** the 4 polarization states should be indistinguishable otherwise we get security loopholes.
  - **Different wavelengths**
  - **Different time emission**
  - **Different intensity**
- **Non periodic drive of the laser introduces power fluctuations between the rounds**



Lowest QBER 2%

Inline configuration

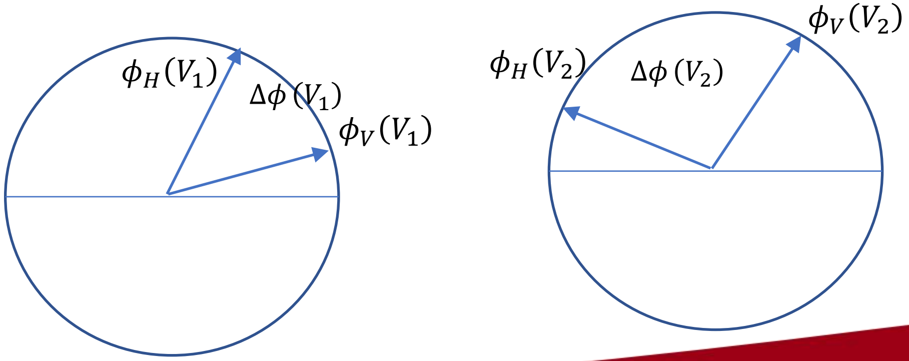
A better, yet simple, solution is to exploit the properties of Z-Cut phase modulators



We recall that Z-Cut phase modulators support two different polarization modes, however they have different modulation efficiencies

For the same modulation voltage the H polarized light will experience a phase retardation of $\phi_H(Volt)$ while $\phi_V(Volt)$. If we enter with a diagonally polarized state: $|\psi\rangle = \frac{1}{\sqrt{2}}(\,|H\rangle + e^{i\phi_0}|V\rangle)$

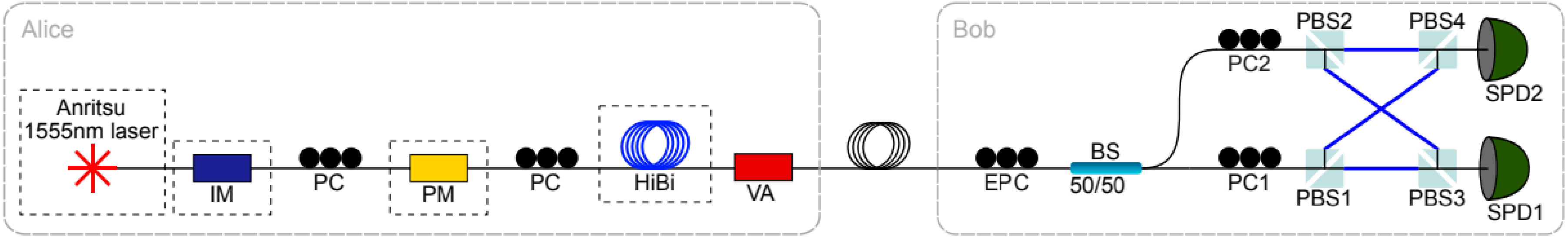
$$\frac{1}{\sqrt{2}}(\,|H\rangle + e^{i\phi_0}|V\rangle) \rightarrow \frac{1}{\sqrt{2}}\left(e^{i\phi_H(Volt)}|H\rangle + e^{i\phi_0+\phi_V(Volt)}|V\rangle\right) = \frac{e^{i\phi_c}}{\sqrt{2}}(\,|H\rangle + e^{i\phi_0+\Delta\phi(Volt)}|V\rangle)$$



By changing the Voltage we can create all the states on the equator of the Bloch sphere

Properties of the inline configuration

This inline configuration is relatively simple to realize either using a PC or twisting the PM fiber at the input of the PM by 45 degree

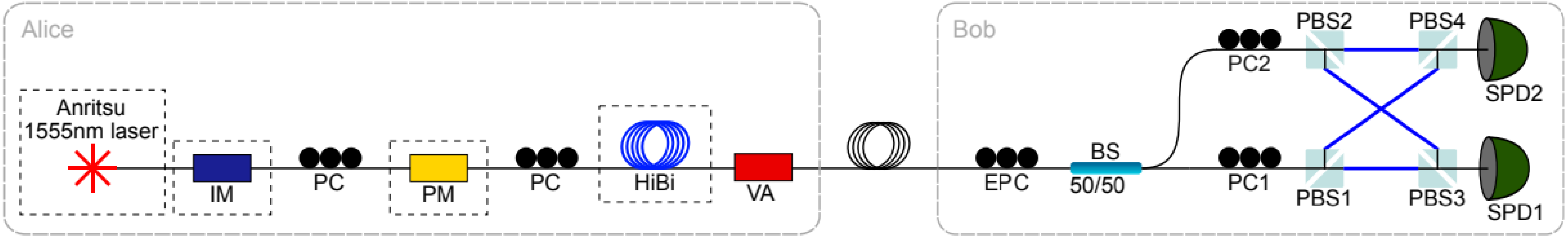


However it has several disadvantages:

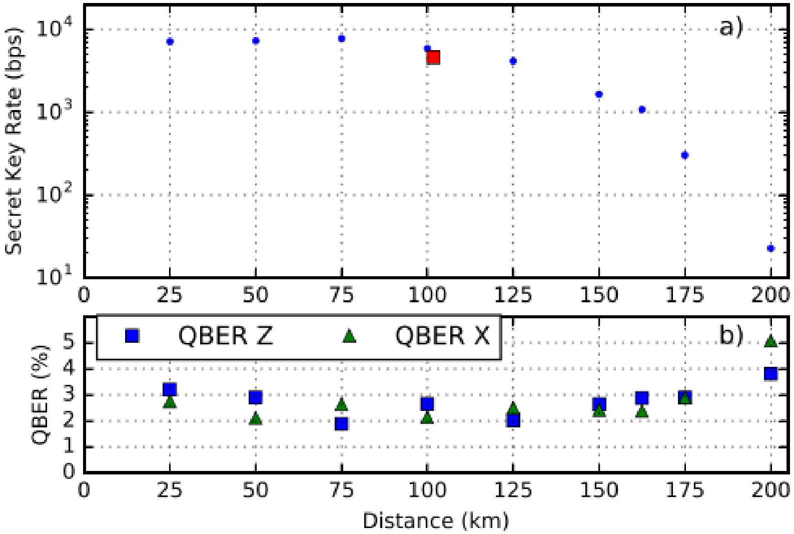
- **Need to control the polarization** at the input of the PM. Any drift of the input polarization will cause a drift of the output polarization. Not only unitary transformation but a change in the relative angles between the states. -> Security issue
- **Phase instability:** any phase instability from the phase modulator will add a term $\phi(t)$ to the relative phase between the polarization. Decrese stability over time
- **Higher modulation voltages:** the polarization modulation is given by the relative phase modulation between the two components. Usually a factor 3 in difference. Need to apply $\frac{3}{2}\pi$ to the phase modulator to obtain a π shift in polarization
- **Polarization mode dispersion:** the PM is long and highly birefringent. The H and V components will travel at different speeds. For short pulses this will add a time-offset to the components that will induce depolarization, increasing the QBER

Performance of the inline configuration

This inline configuration offers limited performances due to the instability problems and the PMD introduced by the modulator



Still relatively high QBER
Around 2%

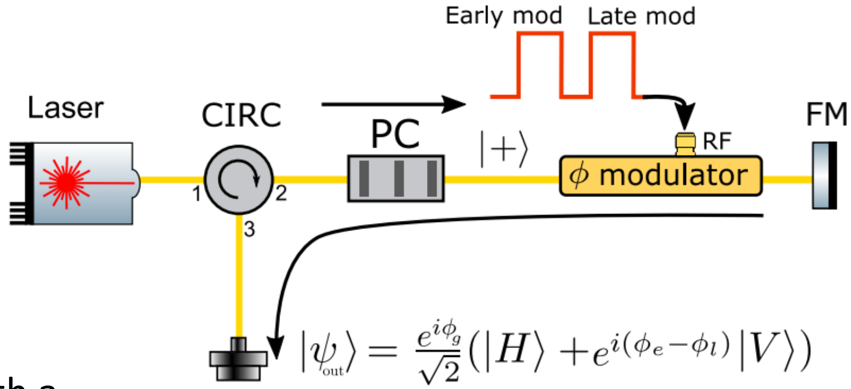


Two way with faraday mirror

An alternative solution is to use a two-way scheme with Faraday mirror

The scheme is similar with the PC prepraring a state before entering in the phase modulator:

$$\frac{1}{\sqrt{2}}(\,|H\rangle + e^{i\phi_0}|V\rangle)$$



$$|\psi_{\text{out}}\rangle = \frac{e^{i\phi_g}}{\sqrt{2}}(|H\rangle + e^{i(\phi_e - \phi_l)}|V\rangle)$$

If we modulate the phase before the reflection with a positive voltage we add a relative phase

$$\frac{1}{\sqrt{2}}(\,|H\rangle + |V\rangle) \rightarrow \frac{e^{i\phi_c}}{\sqrt{2}}(\,|H\rangle + e^{\Delta\phi_e(Volt)}|V\rangle)$$

After the reflection, since the faraday mirror exchanges H and V it becomes a negative phase

$$\frac{e^{i\phi_c}}{\sqrt{2}}(\,|H\rangle + e^{\Delta\phi_e(Volt)}|V\rangle) \rightarrow \frac{e^{i\phi_c}}{\sqrt{2}}(\,|V\rangle + e^{\Delta\phi_e(Volt)}|H\rangle) \rightarrow \frac{e^{i\phi_c + \Delta\phi_e(Volt)}}{\sqrt{2}}(\,|H\rangle + e^{-\mathrm{i}\Delta\phi_e(Volt)}|V\rangle)$$

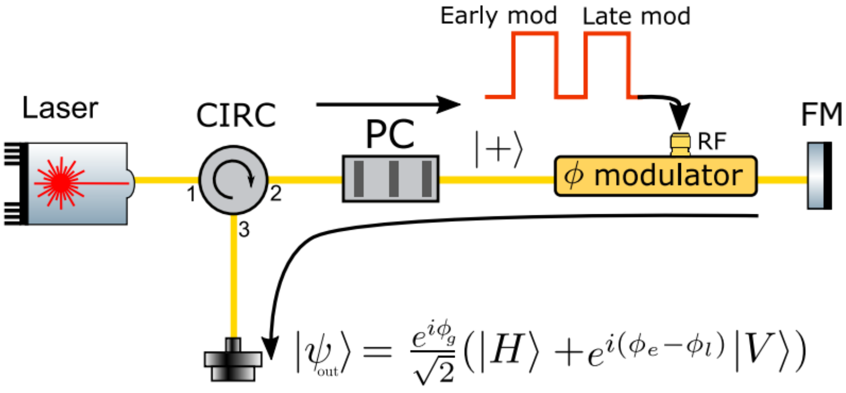
A late modulation, will add a positive phase $\Delta\phi_l(Volt)$ so that together

$$\frac{e^{i\phi_g}}{\sqrt{2}}(\,|H\rangle + e^{\mathrm{i}\,(\Delta\phi_l(Volt) - \Delta\phi_e(Volt))}|V\rangle)$$

Because of this any fluctuation term $\boldsymbol{\Delta\phi_0(t)}$ experienced before and after the reflection will be canceled out!

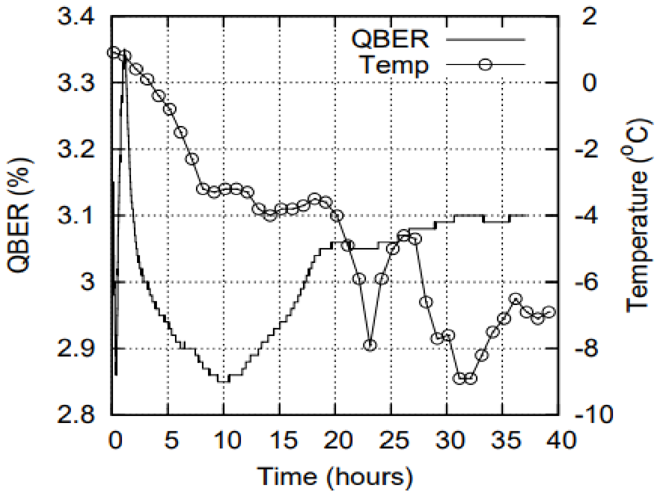
Properties of the two-way with Faraday mirror

The two-way scheme with Faraday mirror has some advantages and disadvantages


Early mod
Late mod
Laser
CIRC
PC
FM
RF
$|+\rangle$
ϕ modulator
1
2
3
$|\psi_{\text{out}}\rangle = \frac{e^{i\phi_g}}{\sqrt{2}}(|H\rangle + e^{i(\phi_e-\phi_l)}|V\rangle)$

PRO:

- **Stability**: it improves the overall stability over time since phase fluctuations are completely canceled out by the Faraday mirror



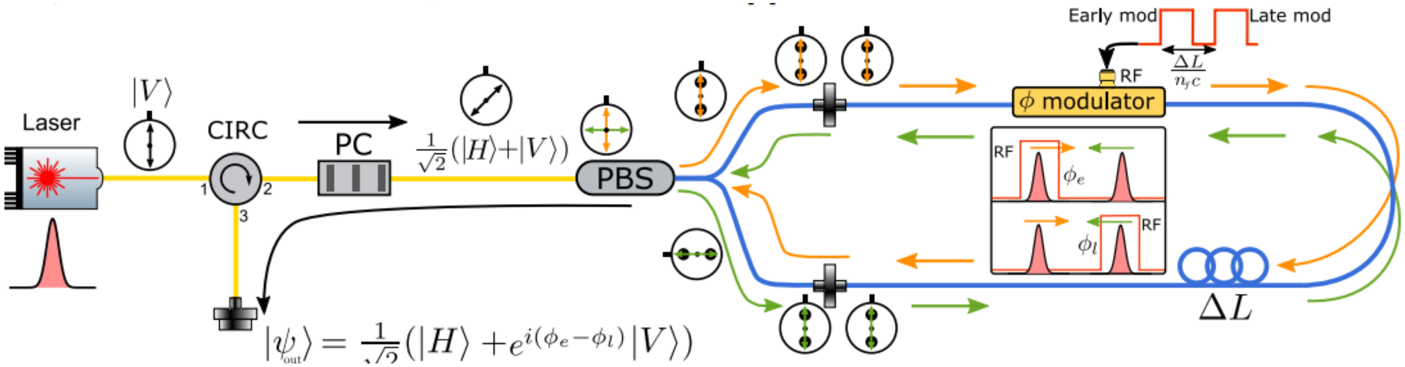
High QBER and low stability

CONS:

- **Polarization**: it still requires a phase modulator supporting both polarizations
- Still requires stabilization of input polarization
- Not all the PMD is compensated
- Still requires high modulation voltages
- Adds timing constraints to the modulation

POGNAC

A method that improves the previous solution is called POGNAC and exploits the properties of Sagnac loop


Laser
$|V\rangle$
CIRC
1
2
3
PC
$\frac{1}{\sqrt{2}}(|H\rangle+|V\rangle)$
PBS
Early mod
Late mod
RF
$\frac{\Delta L}{n_f c}$
ϕ modulator
RF
ϕ_e
RF
ϕ_l
ΔL
$|\psi_{\text{out}}\rangle = \frac{1}{\sqrt{2}}(|H\rangle + e^{i(\phi_e-\phi_l)}|V\rangle)$

Working principle:

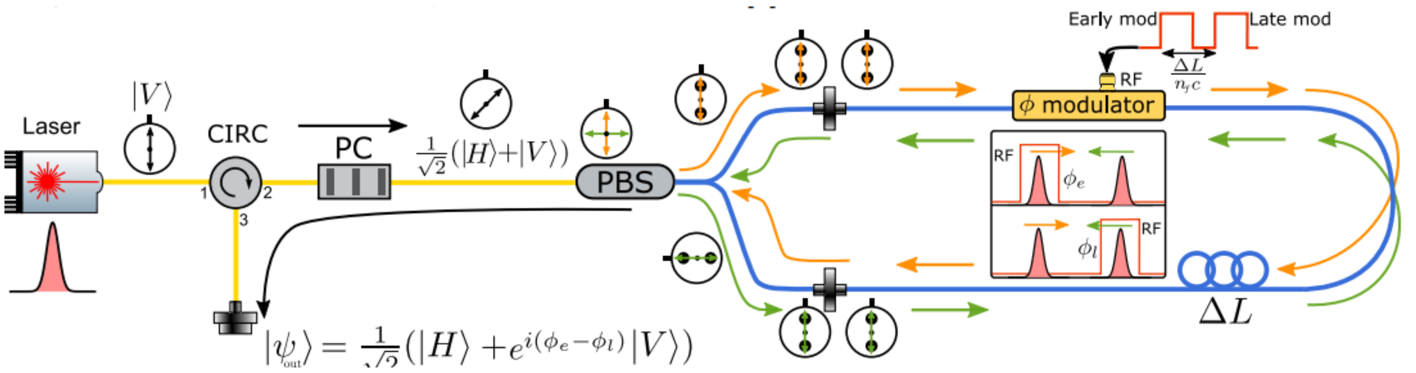
- A PC prepares a balanced superposition of H and V $\frac{1}{\sqrt{2}}(\,|H\rangle + e^{\psi_0}|V\rangle)$
- The PBS splits the two components in the clockwise and counter-clockwise directions
- The output fiber of the PBS on the H axis is aligned with the PANDA and with the key on the horizontal axis. After the connection with the next fiber this map H in V. Now a single polarization runs in the loop.
- The PM is placed asymmetrically and the CW and CCW pulse arrive at different times
- A phase modulation on the early pulse add a positive shift while a late adds a negative shift
- At the PBS after the recombination the state is

$$|\psi_{\text{out}}^{\phi_e,\phi_\ell}\rangle = \frac{1}{\sqrt{2}}\left[|H\rangle + e^{i(\phi_e-\phi_\ell-\varphi_0)}|V\rangle\right]$$

Any common phase fluctuation is canceled out!

Properties of the POGNAC

The POGNAC improves the Faraday Mirror solution, however still has some drawbacks


Laser
$|V\rangle$
CIRC
1
2
3
PC
$\frac{1}{\sqrt{2}}(|H\rangle+|V\rangle)$
PBS
Early mod
Late mod
RF
$\frac{\Delta L}{n_f c}$
ϕ modulator
RF
ϕ_e
ϕ_l
RF
ΔL
$|\psi_{out}\rangle = \frac{1}{\sqrt{2}}(|H\rangle + e^{i(\phi_e-\phi_l)}|V\rangle)$

PRO:

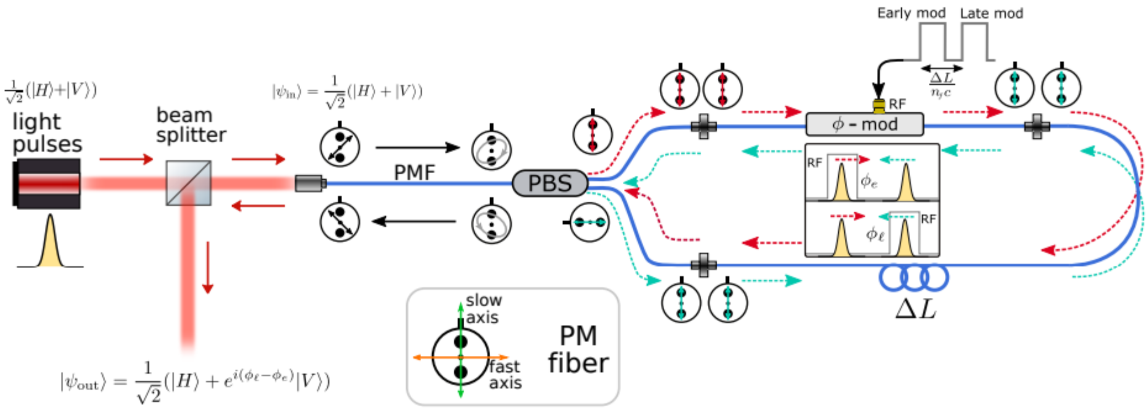
- **Stability:** phase fluctuations longer than a round trip are canceled out
- Only one polarization runs in the loop: no need of special PM
- Since only one polarization PMD is completely compensated –> high ER
- Lower modulation voltages: phase modulation is directly mapped ad voltage modulation

CONS:

- Still requires stabilization of input polarization
- Adds timing constraints to the modulation
- Unknown polarization state at the output due to SMF

IPOGNAC

To solve the problem of input polarization and known output states we can use the IPOGNAC



$\frac{1}{\sqrt{2}}(|H\rangle+|V\rangle)$
light pulses
beam splitter
$|\psi_{\text{in}}\rangle = \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle)$
PMF
PBS
Early mod
Late mod
$\frac{\Delta L}{n_g c}$
RF
ϕ - mod
RF
ϕ_e
RF
ϕ_ℓ
ΔL
slow axis
fast axis
PM fiber
$|\psi_{\text{out}}\rangle = \frac{1}{\sqrt{2}}(|H\rangle + e^{i(\phi_\ell - \phi_e)}|V\rangle)$

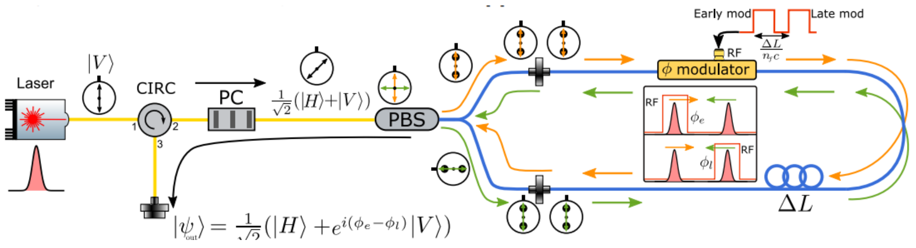
Similar working principle:

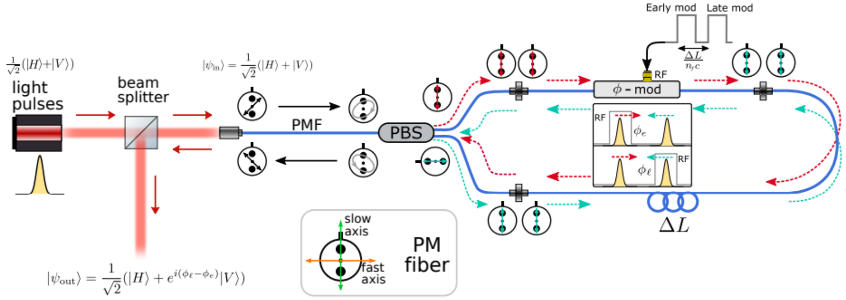
- Input free-space BS and light coupled @45 degree in the input fiber
- Input PM fiber instead of SM. In general between the coupler and the PBS the light will pick up a relative phase ϕ_i
- However, since also the Sagnac loop exchanges H with V, this ϕ_i phase will be compensated in the way back
- At the output of the BS in reflection we have known state of polarization, since there are no unitary transformations applied by the SM fiber and the input relative phases are compensate

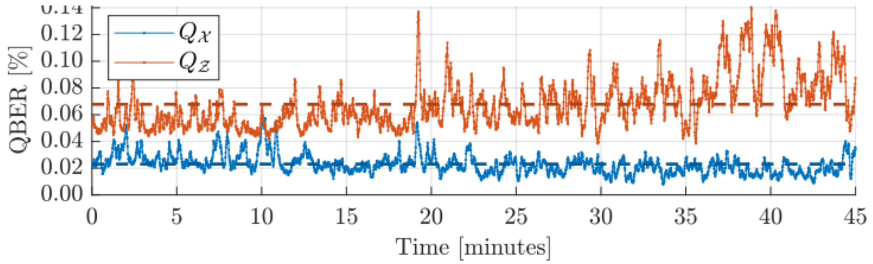
Solves problems of input stability and output reference, useful for free-space

Performance of POGNAC and IPOGNAC

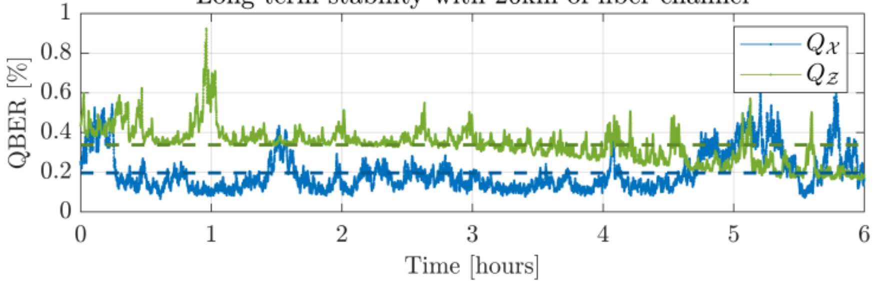
The removal of the PMD and the increased stability allow for a substantially lower QBER


Laser
$|V\rangle$
CIRC
PC
1
2
3
$\frac{1}{\sqrt{2}}(|H\rangle+|V\rangle)$
PBS
Early mod
Late mod
RF
$\frac{\Delta L}{n_f c}$
ϕ modulator
RF
ϕ_e
ϕ_l
RF
ΔL
$|\psi_{\text{out}}\rangle = \frac{1}{\sqrt{2}}(|H\rangle + e^{i(\phi_e-\phi_l)}|V\rangle)$

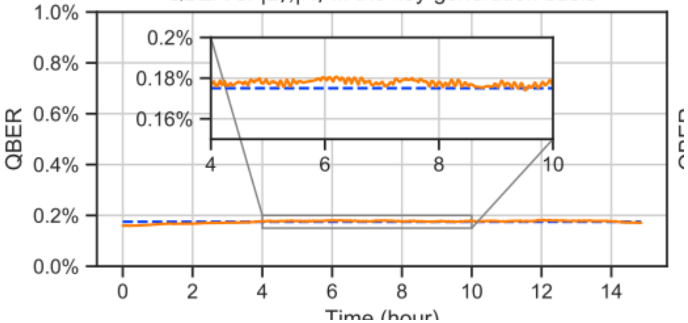

$\frac{1}{\sqrt{2}}(|H\rangle+|V\rangle)$
light pulses
beam splitter
$|\psi_{\text{in}}\rangle = \frac{1}{\sqrt{2}}(|H\rangle+|V\rangle)$
PMF
PBS
Early mod
Late mod
RF
$\frac{\Delta L}{n_f c}$
ϕ - mod
RF
ϕ_e
ϕ_ℓ
RF
ΔL
slow axis
fast axis
PM fiber
$|\psi_{\text{out}}\rangle = \frac{1}{\sqrt{2}}(|H\rangle + e^{i(\phi_\ell-\phi_e)}|V\rangle)$



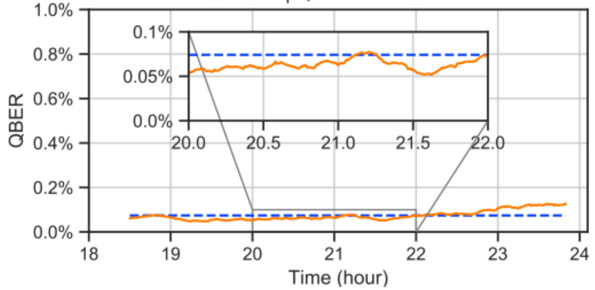
Long term stability with 26km of fiber channel



QBER of |L⟩,|R⟩ in the key-generation basis



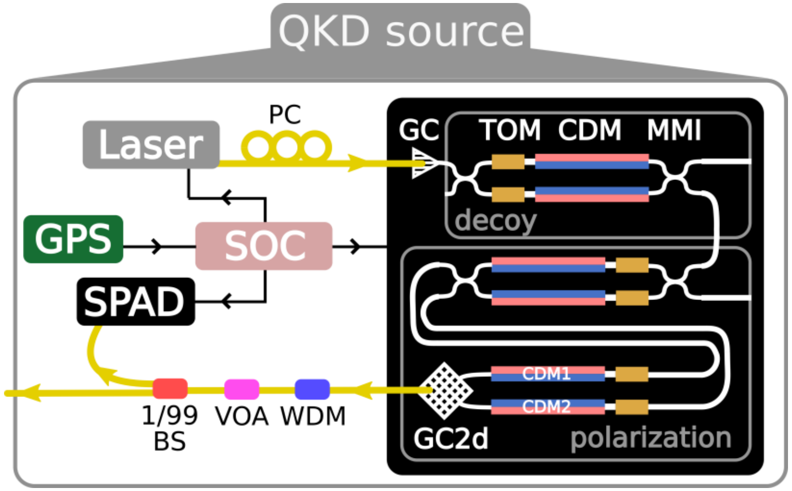
QBER of |D⟩ in the check basis

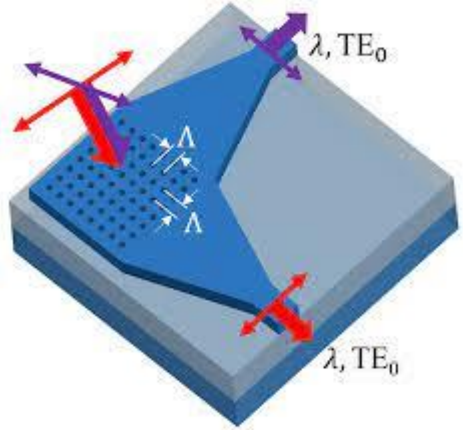


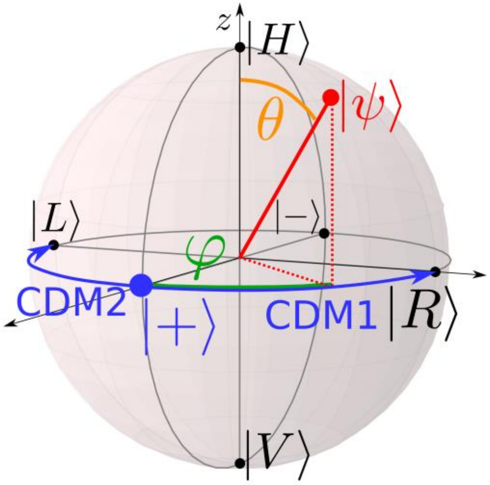
Qber below 0.05%

What about integrated optics?

A common problem in silicon photonics is that silicon waveguides support only one polarization. Can we still have polarization-encoded QKD?







The idea is to use only one polarization and map two different paths to different polarizations.
The Grating Coupler 2D maps two TE modes, with orthogonal input into orthogonal polarizations

Then, using the structure in the picture:

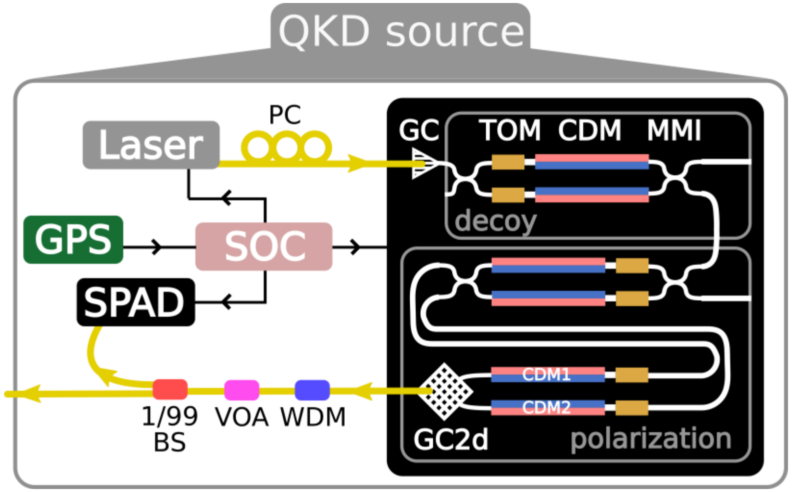
- First MZI used for intensity modulation
- Second MZI allows to prepare light all in the upper arm (H pol) or in the lower (V pol) or a linear combination. This allows to move up or down in the bloch sphere
- The last set of phase modulators allow to add a relative phase to H, or V. If enter with a |+> state allows to generate L or R

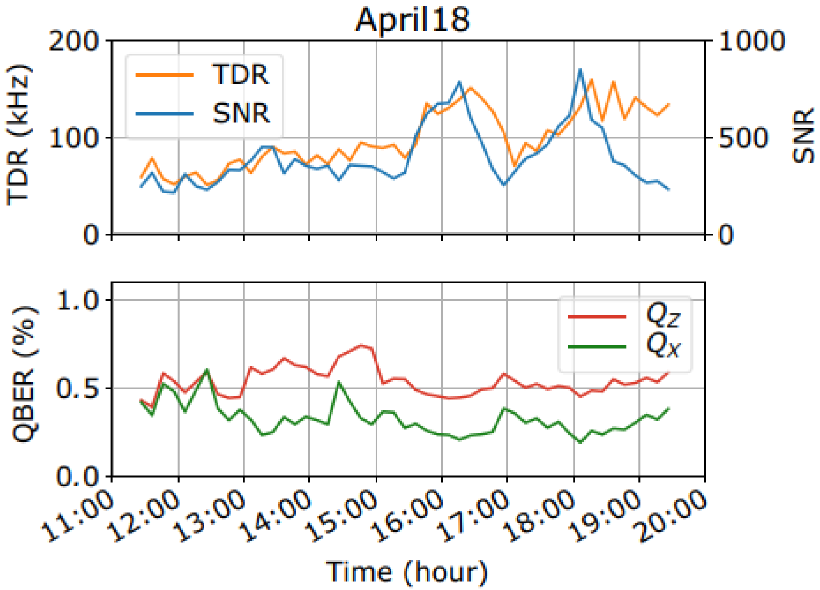
Moving on the equator of Bloch

Performance of the Integrated polarization QKD

The integrated solution, while being an interferometric structure offers a reasonable high stability due to the integration of all components in the same substate and small length at play

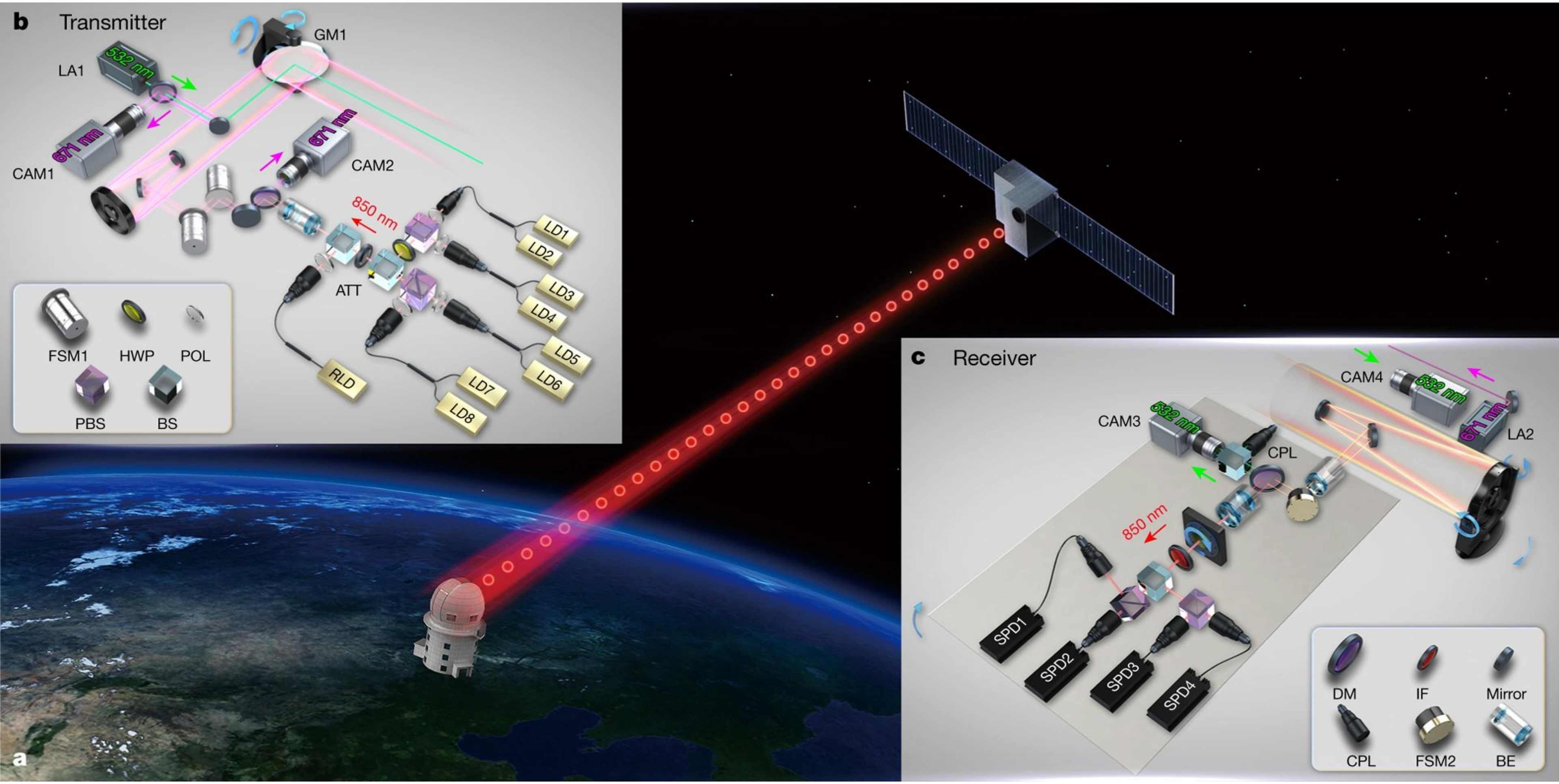
Also, only one polarization is present in the chip allowing to remove PMD and achieving low QBER





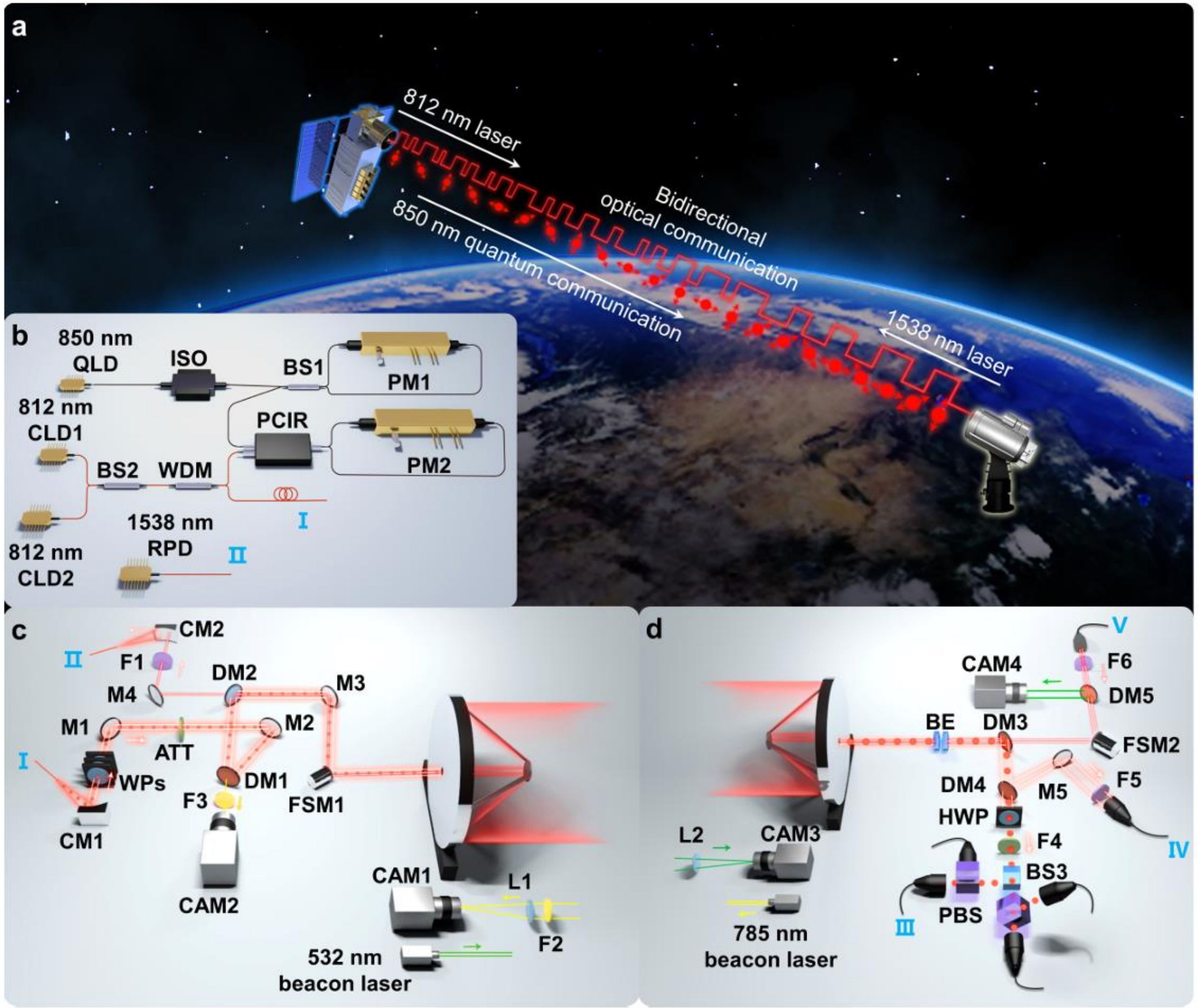
QBER below 0,5% in the free-space implementation in daylight

Satellite QKD source: Micius



Liao, SK., Cai, WQ., Liu, WY. et al. Satellite-to-ground quantum key distribution. Nature 549, 43–47 (2017).

Satellite QKD source: Jinan-1 microsatellite



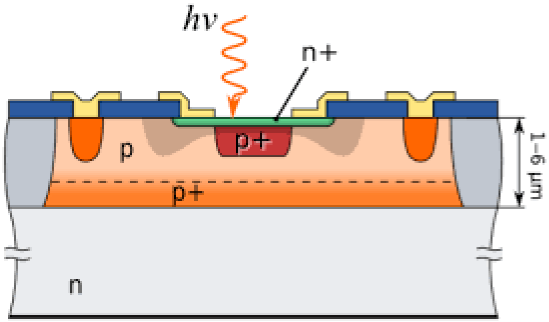
arXiv preprint arXiv:2408.10994

Receivers

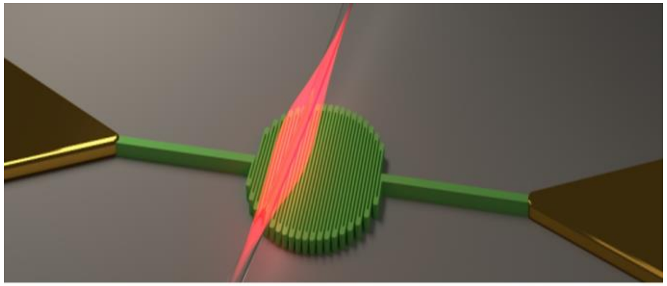
Detector and technologies

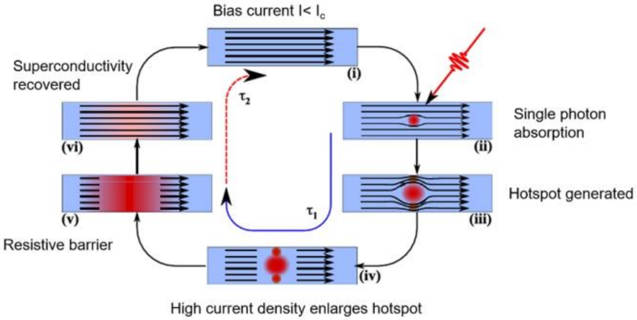
There are two main categories of single photon detectors that are used in usual QKD systems.

Single photon avalanche photodiodes (SPAD)



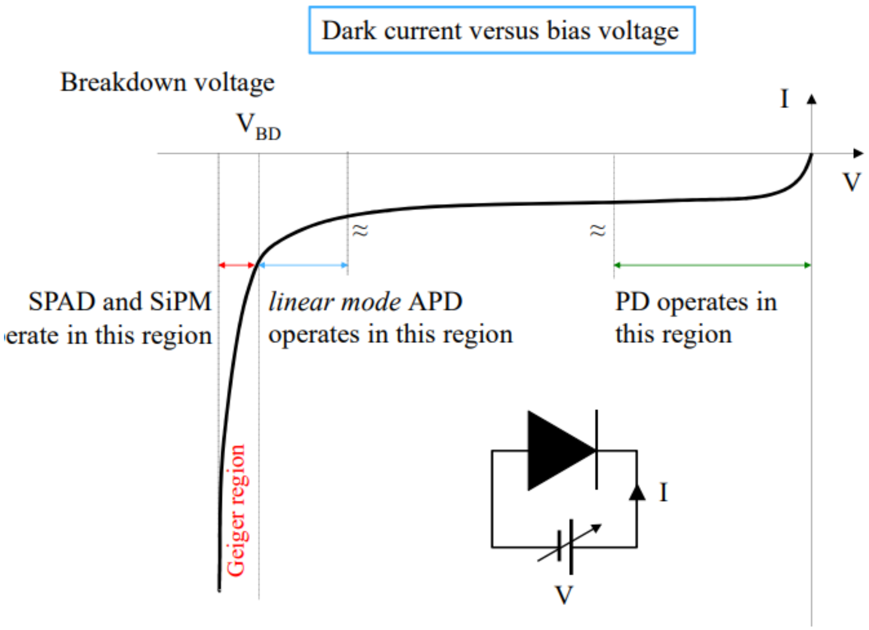
Superconducting Nanowire Single photon detectors (SNSPD)

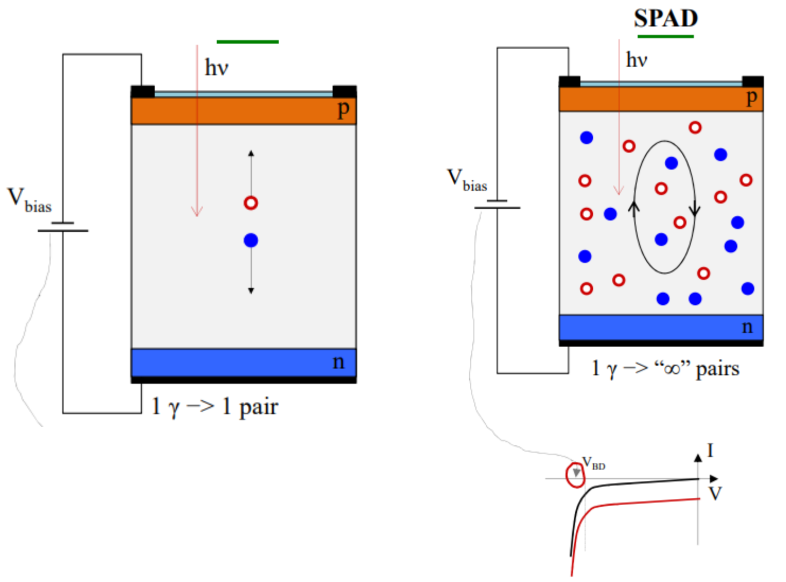




SPAD

The SPAD, as the name says, are similar to conventional PIN diodes, but with a biasing field close the breakdown voltage of the junction



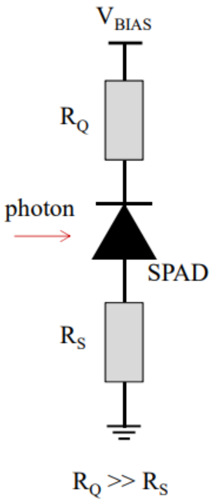


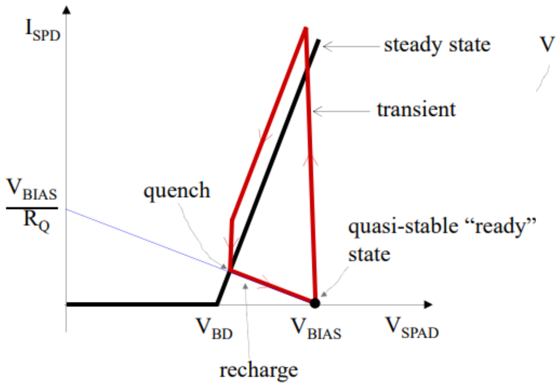
Operation mode of an (A)PD

The photon when interacts with the intrinsic region creates an electron-hole pair that is accelerated by the electric field. In Geiger mode the carriers acquire sufficient kinetic energy that when they collide with the lattice they have energy to create other elector hole pairs, generating an avalanche, and so a macroscopic current.

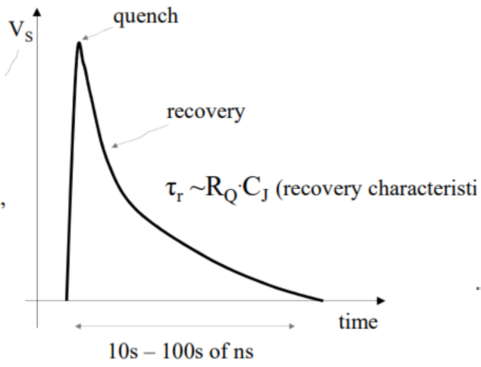
SPAD: quenching

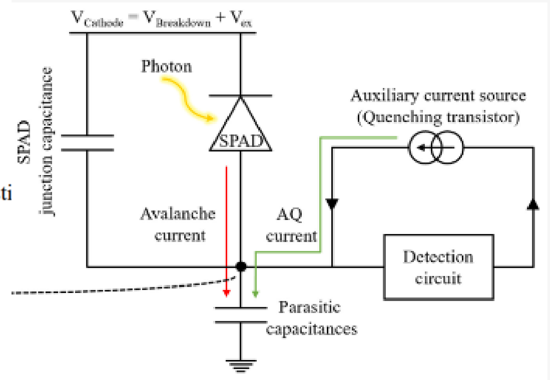
The avalanche is an exponential process, if not blocked will blow up the semiconductor: need to quench the avalanche!





Voltage pulse on R_s due to avalanche





$V_{Cathode} = V_{Breakdown} + V_{ex}$
Photon
SPAD
Auxiliary current source (Quenching transistor)
SPAD junction capacitance
Avalanche current
AQ current
Detection circuit
Parasitic capacitances

Passive quench

Active quench

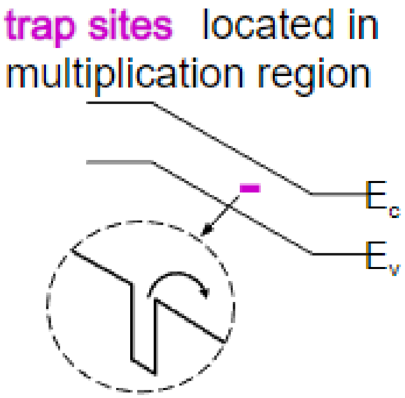
In the passive quench, a large Resistor RQ is used to reduce the voltage bias when the avalanche starts. Such circuits passively quench the circuit.

Drawbacks? Large RQ increases the recovery time!

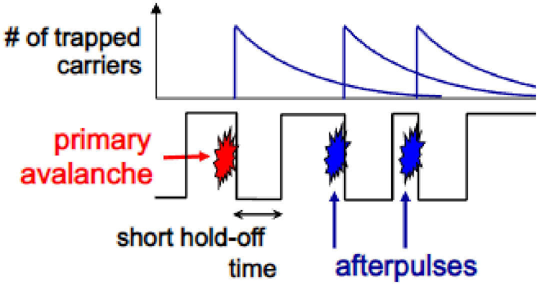
Active quench is faster

SPAD: afterpulse

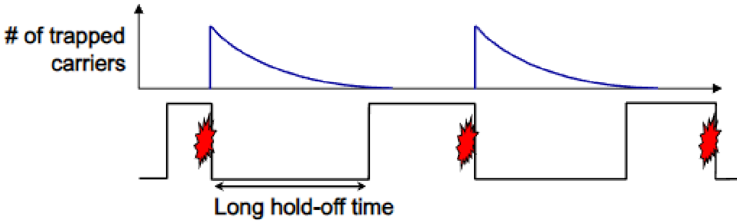
One of the unwanted effects of Spad is the aferpulsing effect:



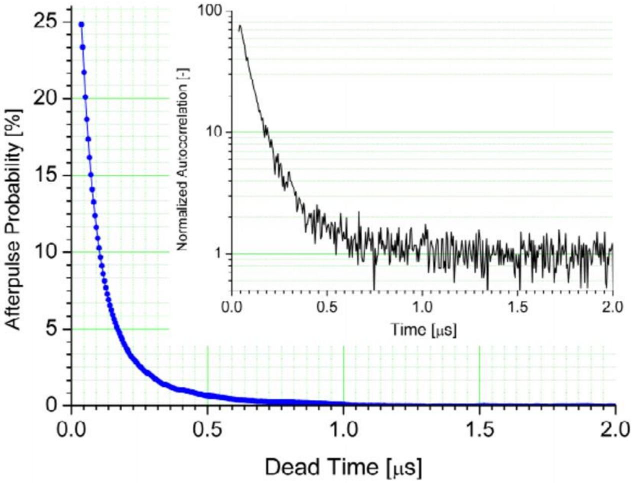
Due to non-perfect purity there are trap levels in the semiconductor



Long decay times. If bias is re-applied trapped electrons or holes start the avalanche!



Need to increase the holdoff-time to avoid avalanche

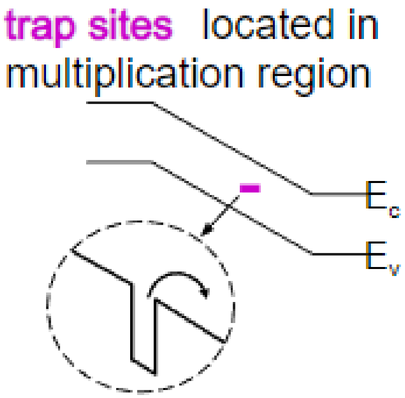


- The higher the avalanche the higher the afterpulse.
- The shorter the holdoff the higher the afterpuse
- The lower the spad temperature, the higher the lifetime of trap states, the higher the afterpulse
- For Si, DT=1us, for InGAs DT=10-40us

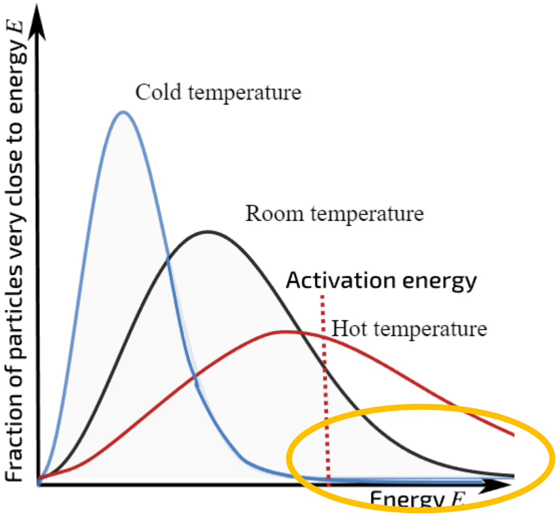
Main limitation to high count-rate SPAD

SPAD: dark counts

Another unwanted effect is due to dark counts detections



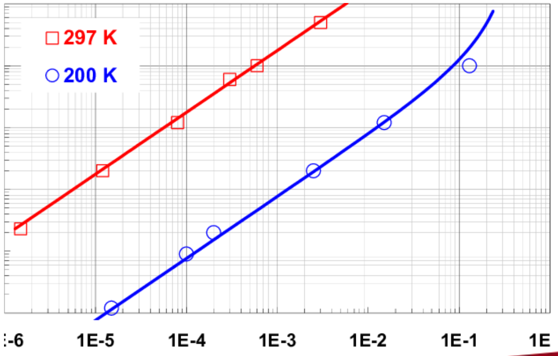
The energy gap between the conduction and the valence band is finite



Carriers in the SPAD are at a non-zero temperature and their energy is distributed as a Maxweel-Boltzmann distribution

Due to the long tail at high energy, statistically some carrier will have the energy to "jump" starting the avalanche

This problem is more severe in InGAs where the energy gap is smaller that in silicon where the gap is bigger

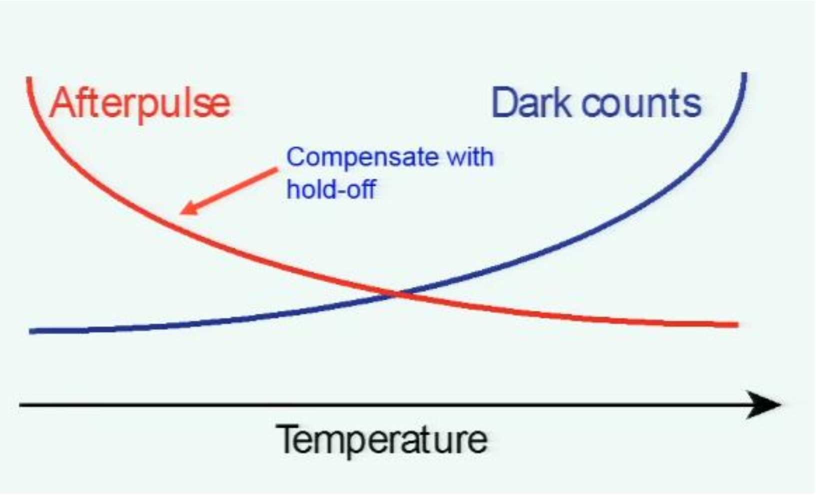


Solutions:

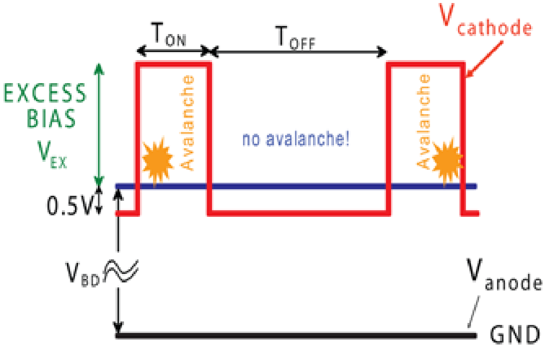
- Cool down the SPAD
- Cool down the fiber
- Decrease the bias

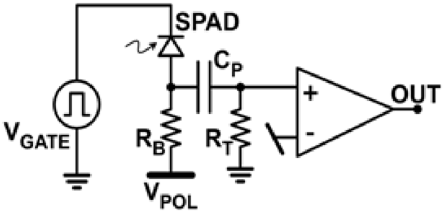
SPAD: afterpulse and dark counts and gating

However cooling down increase the holdoff!



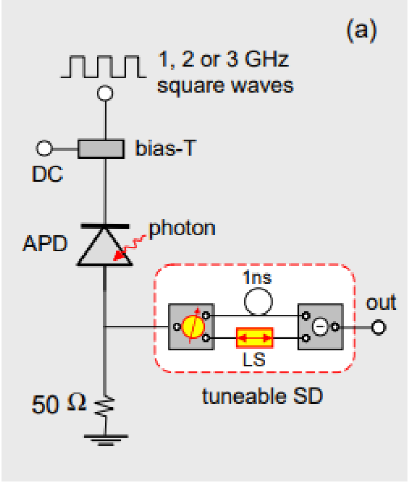
Another method: gating!

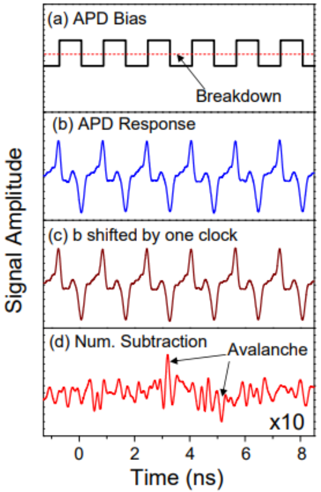


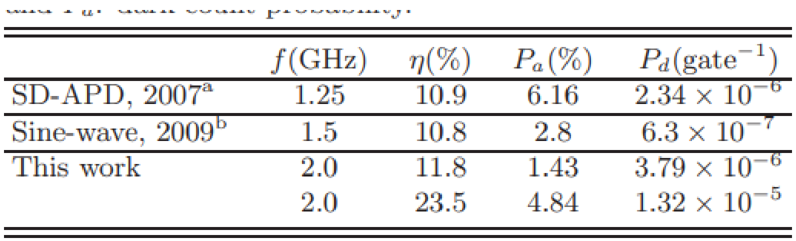


Only turn on bias for short time, when you expect the photon. Need good synchronization!

An option is to use Self-Differenciating detectors!







and P_d: dark count probability.

	f(GHz)	η(%)	P_a(%)	P_d(gate^{-1})
SD-APD, 2007[a]	1.25	10.9	6.16	2.34×10^{-6}
Sine-wave, 2009[b]	1.5	10.8	2.8	6.3×10^{-7}
This work	2.0	11.8	1.43	3.79×10^{-6}
	2.0	23.5	4.84	1.32×10^{-5}

- GHz square waves to gate
- Small excess bias -> smaller avalanche
- Shorter avalanche
- SD circuit reveals avalanche over capacitive transient

Typical SPAD performances

Let’s summarize the typical SPAD performances

Silicon:

- Detection efficiency@800: 62%
- Dark counts: 100-1500 cps
- Jitter: 350ps
- Dead time: 40ns

InGAs

- Detection efficiency@1550: 15-25%
- Dark counts: 1-10k cps
- Jitter: 70 - 200 ps
- Dead time: 10 – 100 us

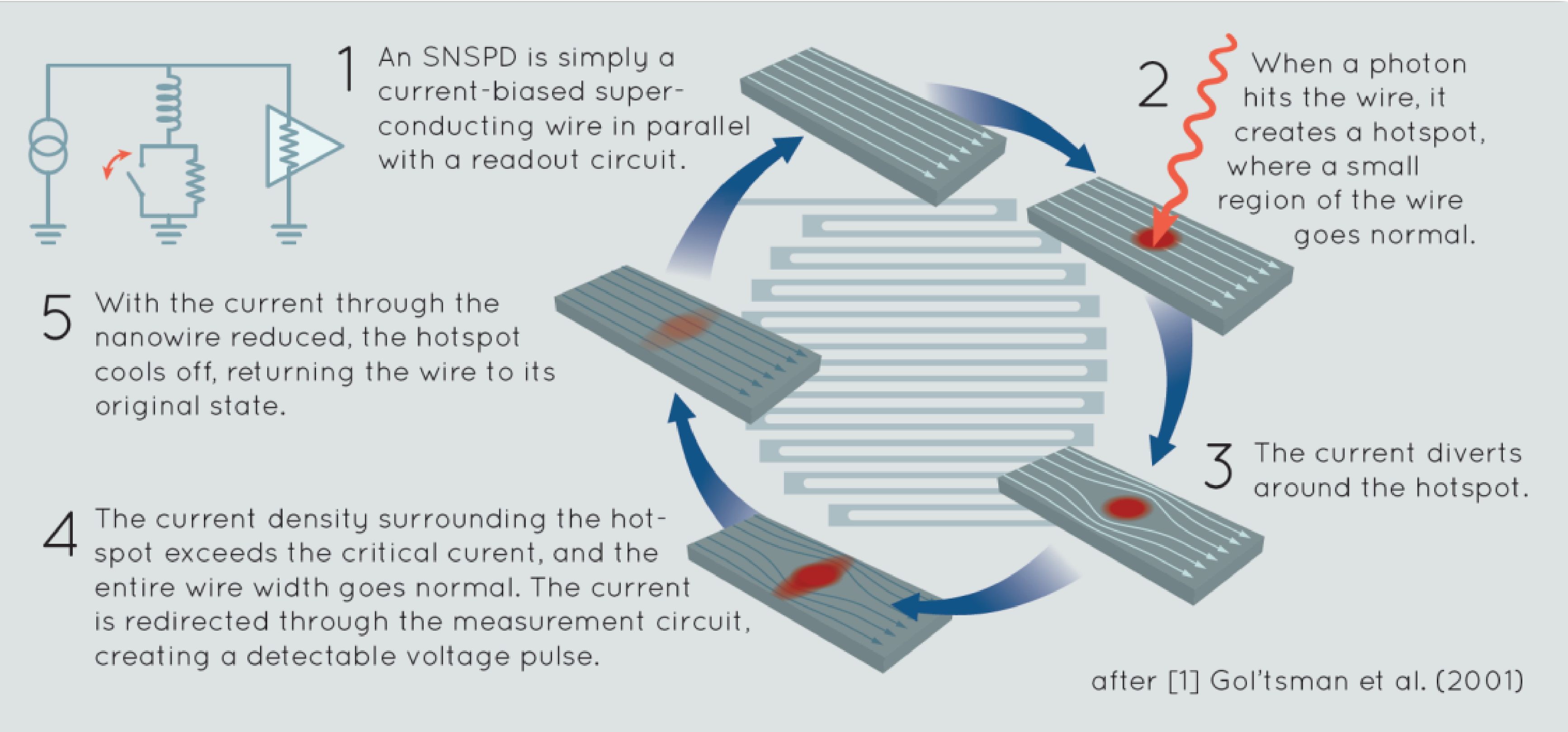
Self-Differentiating

- Detection efficiency@1550: 15-25%
- Dark counts: 3k cpg
- Jitter: 100 ps
- Dead time: 0.5 - 1 ns

SNSPD

The other technology is given by SNSPD:

Working principle



1 An SNSPD is simply a current-biased superconducting wire in parallel with a readout circuit.

2 When a photon hits the wire, it creates a hotspot, where a small region of the wire goes normal.

3 The current diverts around the hotspot.

4 The current density surrounding the hotspot exceeds the critical curent, and the entire wire width goes normal. The current is redirected through the measurement circuit, creating a detectable voltage pulse.

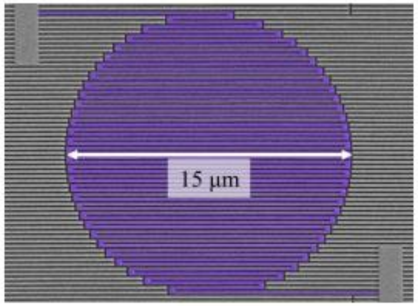
5 With the current through the nanowire reduced, the hotspot cools off, returning the wire to its original state.

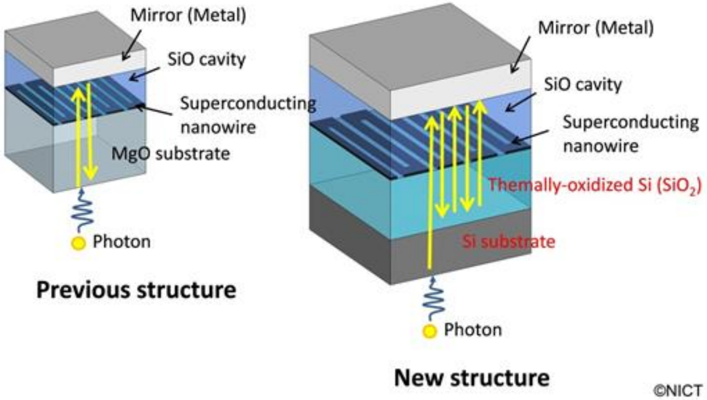
after [1] Gol'tsman et al. (2001)

SNSPD: requirements

Requirements and properties:

- Different superconducting materials NbN, Wsi but all require cryostat, vacuum and cooling: 0,8 – 3,5K
- Up to now dimension is around 15um or smaller: need to couple ino SM fibers not MM
- Polarization dependent: due to asymmetry one polarization has higher absorption than the other (half)
- Cavity: SNSPD are broadband but to enhance efficiency they have a cavity specific for the wavelength of interest



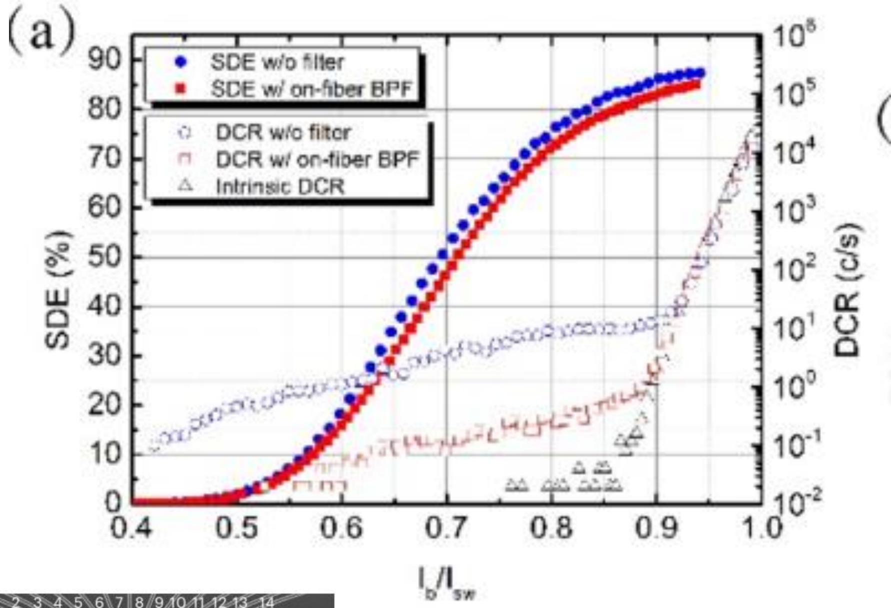


©NICT

SNSPD: performances

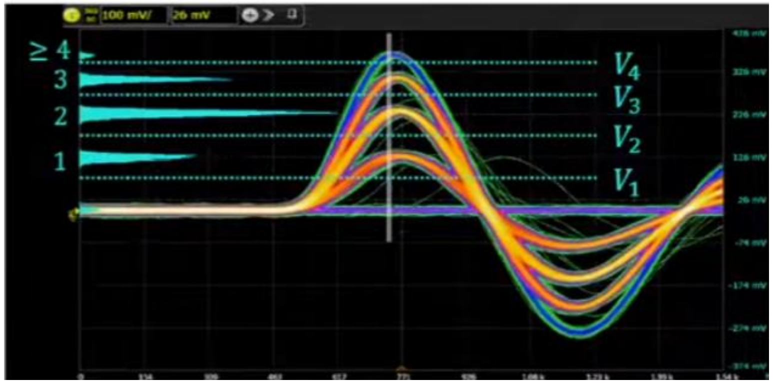
Typical performances of SNSPD:

- Efficiency @ 1550nm: up to 99%, typical 85%
- DCR: down to 0,1cps, typical 100cps
- Jitter: down to 10ps, typical 50-100ps
- Recovery time: 10 to 100ns @50%

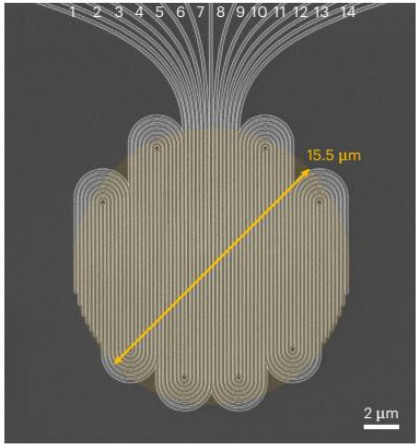


Other features:

Photon Number resolving



Different amplitudes for different number of resolved photons

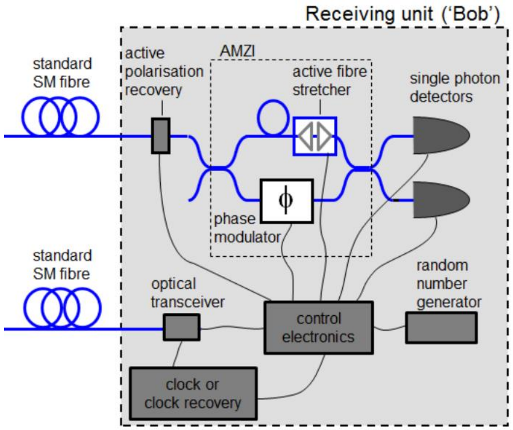


Multi pixel SNSPD

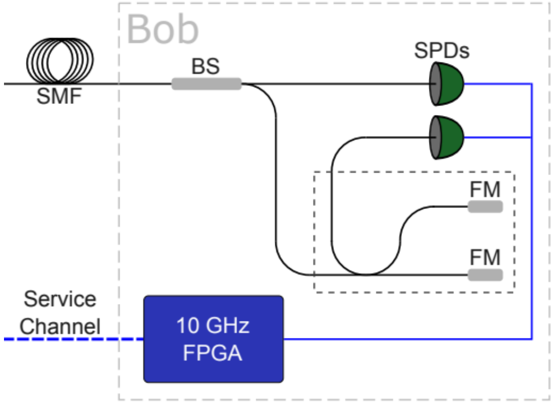
360 Mcps!

Receivers

Let’s look now at the receiver side. The setup are similar for phase and time-bin



Phase receiver



Time-bin receiver

The main issue for both setup is that they involve interferometers for the extraction of the relative phase between the time bins.
As we have seen, interferometers suffer from stability issues over time due to their sensitivity to environmental factors such as temperature.

Additional challenge: to obtain good visibilities the delay of the transmitting IF should match as much as possible the one at the receiver.

- We recall that 1ns delay is around 20cm in fiber. Pulses are usually 30ps large, a precision of 10ps is 2mm
- Also the phase reference should match: when

Alice send 0 phase, constructive IF

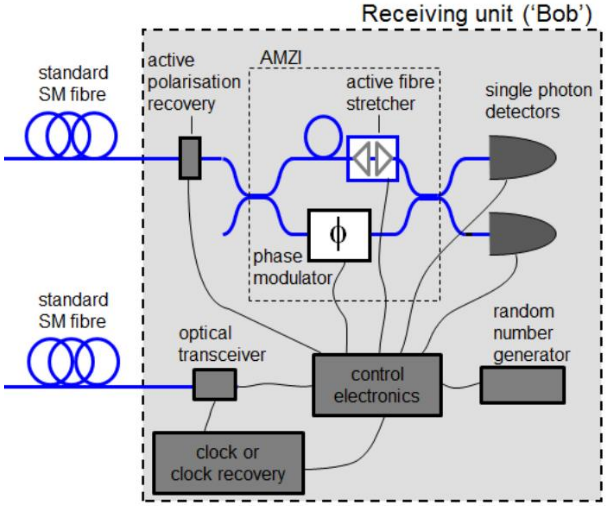
Phase receiver

Let’s look at the phase receiver:

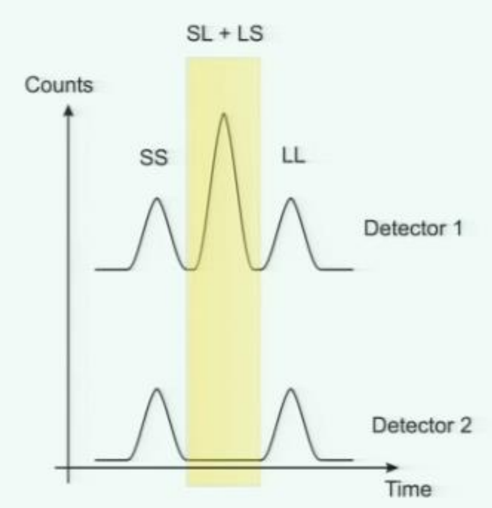
- Polarization recovery to fix the pol at the receiver
- When the state $\frac{1}{\sqrt{2}}(||e\rangle + e^{i\phi}|l\rangle)$ enters in the AMZI

We have 4 possible outputs: Short-Short, Long-Long, Short-Long, Long-Short. Only last two give rise to interference

- Postselect only the central peak.
- Click in the upper detector: 0 phase, lower, π phase
- The PM is used to add $\frac{\pi}{2}$ phase when measuring in the check basis



Phase receiver



Several important points:

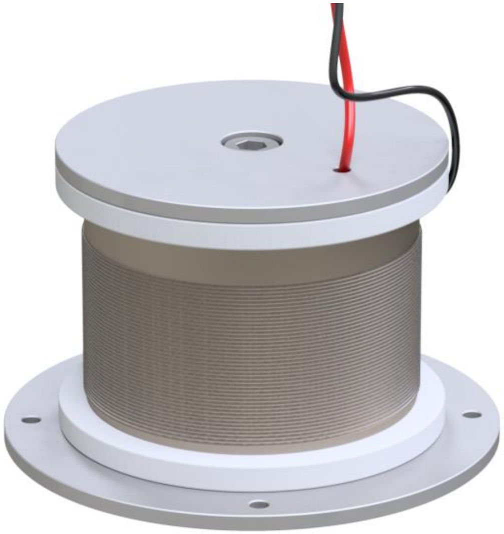
- Relative length difference between trasmitter and receiver may change over time. Use fiber stretcher to adjust
- Relative phase may change: use a dc offset with the phase modulator to adjust the steady phase of the interferometer
- These changes are fast! Either use a second wavelength or fast data from the check basis (public)
- Active basis selection! Uses randomness and requires good synchronization!

Fiber stretcher

Just a couple of words on Fiber stretcher:

When one needs to change the length of the fiber by more than one or two wavelenghts, phase modulators are not suitable.

Fiber stretchers are piezoelectric elements with fiber coils attached. They phisically compress or elongate the fiber, increasing the delay.



Few characteristics:

- Delay range: 8 π up to ps
- Voltage: usually require 100V to drive (piezo)
- Speed: from few Hz up to tens of kHz
- Low loss: <1db

Main problems:

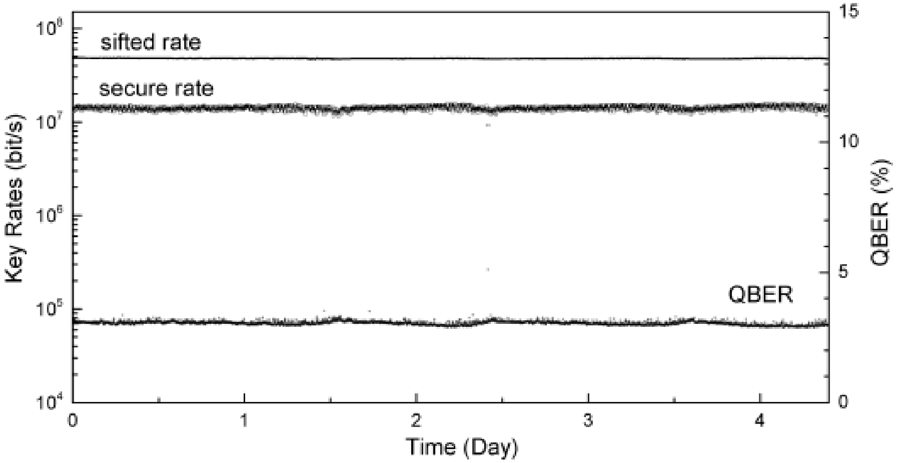
- Add fiber in the loop increasing the instability
- Hysteresis: after tuning the device the fiber require some time to relax, creating drifts in the phase during the transient

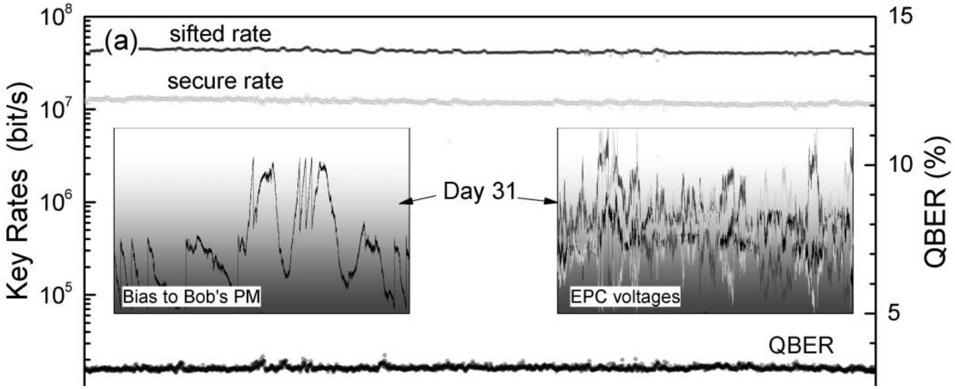
Phase receiver typical performances

By looking at the performance over time:

- QBER is quite symmetric in the key and check basis.
- Visibilities can be quite high> 99%
- Main contribution to the QBER is the stabilization of phase and length of interferometers
- Drifts in the phase can be fast
- Typical QBER in the order of 2-4% close to saturation

- For synchronization another service channel is required
- Half of pulses lost due to no interference

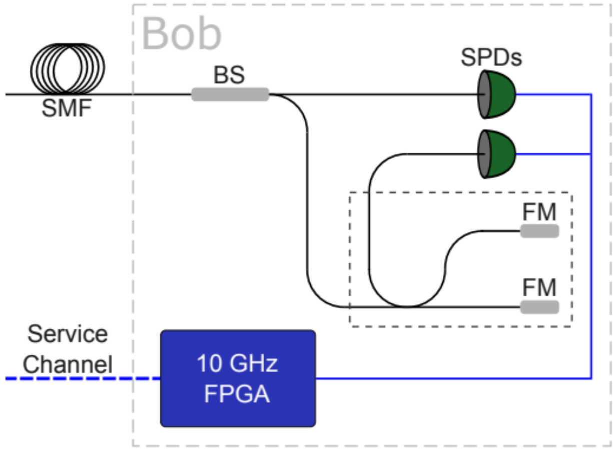




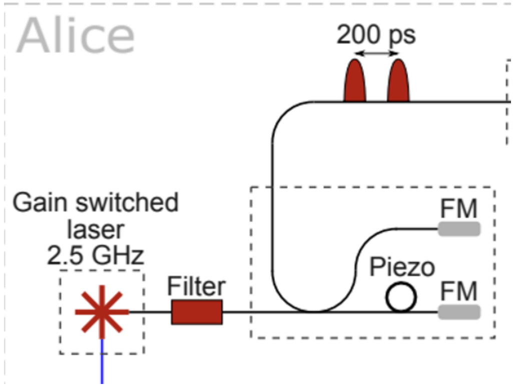
Time-bin receiver

Let’s look at the time-bin receiver:

- The BS selects passively the measurement basis
- One directly sent to a SPD. Measurement in the Key Basis
- Time-measurement tells if received is $|e\rangle$ or $|l\rangle$
- The second branch uses a MF IF to measure the phase without the need of polarization compensation.
- In this case the relative phase is tuned using the piezo at the trasmitter to have destructive IF at the detector
- Also in this case only interference peak is kept



Time-bin



Several advantages:

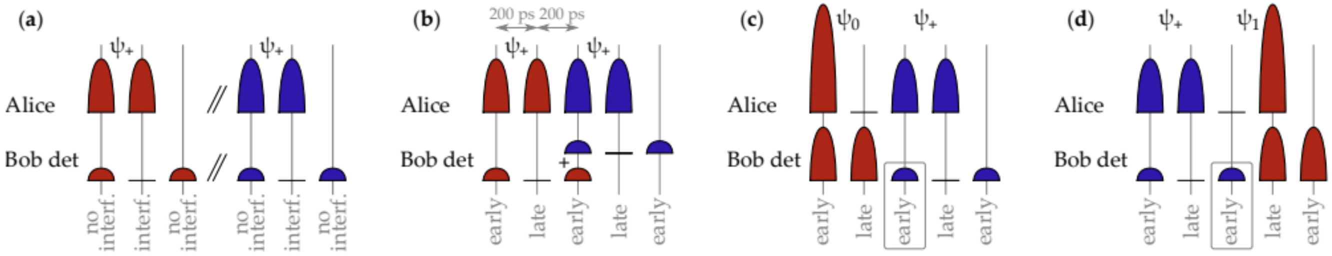
- No active polarization compensation using the FM
- Passive basis selection
- Only one interferometric measurment in the check basis
- All tuning done at the trasmitter (lower losses)

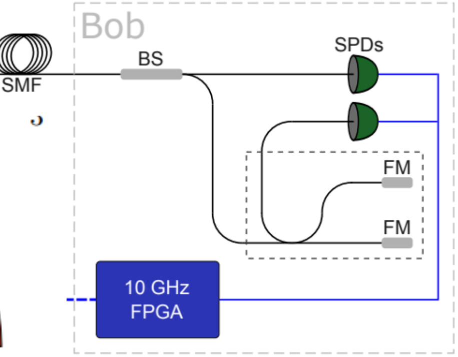
Caveats:

- With only two detectors, need to bound check events from early-early detections

Time-bin receiver with two detectos and overlap

For this specific type of time bin receiver with two detectors we have to estimate the total number of counts.





Not all the events can be used due to estimate this quantity! If pulse separation matches with repetition rate there are correlations between different pulses.

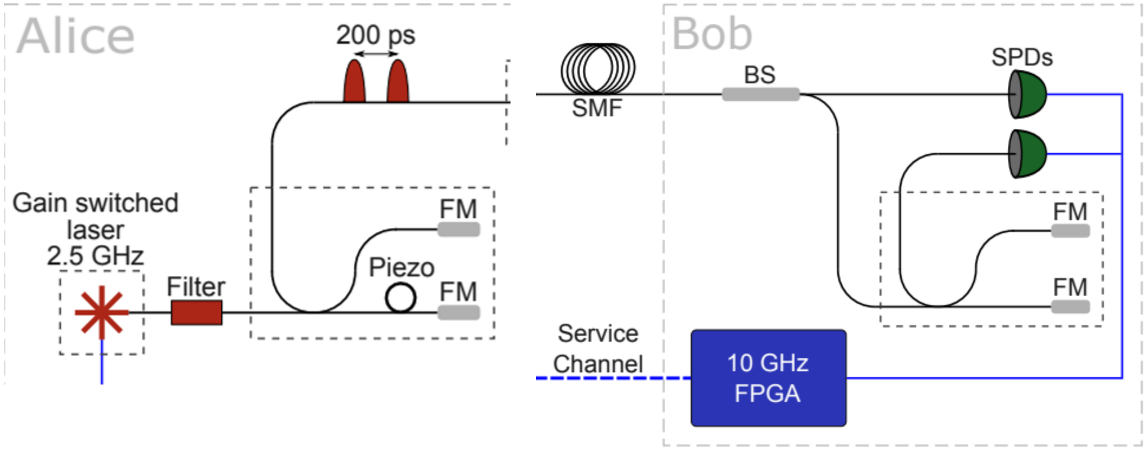
Only events where $|0\rangle$ is followed by $|+\rangle$ or $|+\rangle$ is followed by $|1\rangle$ do not carrry any interference and can be used for the estimation

In the end we get $n_{\mathrm{X}} = \frac{n_{\mathrm{Xside}}}{\frac{1}{4} p_{\mathrm{Z}}^{\mathrm{A}}}.$ where nXside are these measured events, P_z is the probability to send a state in the Z basis. The other factor ½ is because half of the events are going back to the input

Stabilization of the time-bin receiver

In the time-bin receiver the receiver interferometer needs to be stabilized over time.

Only the Check basis needs to be stabilized and the information of the check basis is public so it can be disclosed.

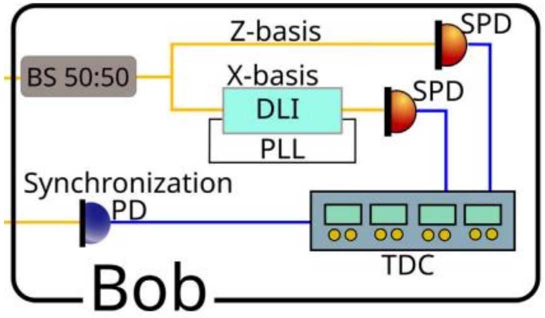


Time-bin

However the main limitation is the time to get a sufficient statistic on from the count rates to evaluate the QBER.

For schemes where the correction is at the trasmitter we have to add the latency of the reconciliation.

Another option is to inject light at a different wavelength in the interferometer and use this wavelength to lock with a PLL the working point of the interferometer. This has to be done for the two interferometers independently.



The second wavelength adds noise to the QBER

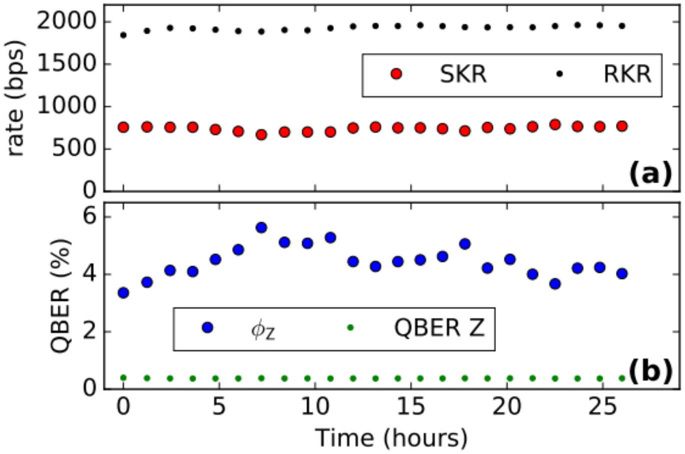
Performances of time-bin receiver

Let’s look at the performances of time-bin receiver:

length (km)	attn (dB)
251.7	42.7
302.1	51.3
354.5	60.6
404.9	69.3
421.1	71.9

QBER Z (%)	ϕ_Z (%)	RKR (bps)	SKR (bps)
0.5	2.2	$12 \cdot 10^3$	$4.9 \cdot 10^3$
0.4	3.7	$1.9 \cdot 10^3$	$0.79 \cdot 10^3$
0.7	1.8	117	62
1.0	4.3	17	6.5
2.1	12.8	2.3 (4.5*)	0.25 (0.49*)

- Asymmetric QBER for Key and Check
- Key error way lower: main source of error finite extinction ratio of IM at the trasmitter side
- Check basis error higer and more unstable: need to perform an interferometric measurement

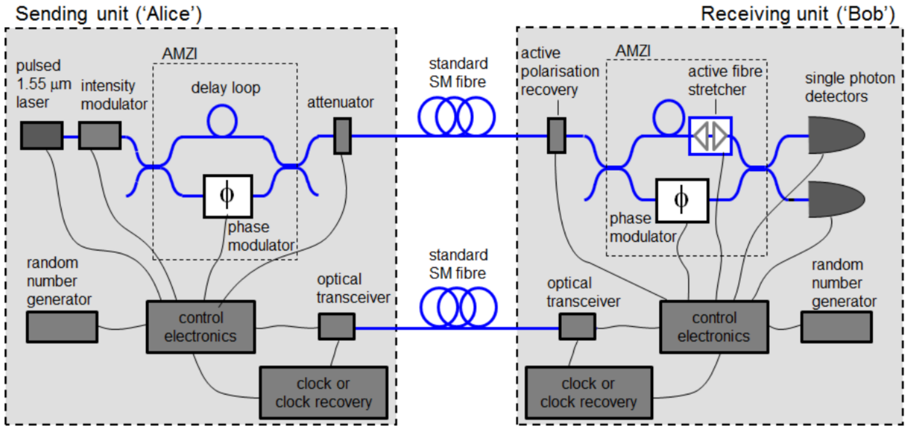


Caveats:

- Need to wait for the reconciliation to perform the stabilization on the phase of the trasmitter interferometer
- Still need to throw away some data not in the interference peak for the check basis

Bandwidth and latency considerations

In a real QKD protocol we have to take into account some considerations about required bandwidth and latency



At the trasmitter side:

- **QRNG:** need at least 1 bit for state, 1 bit for basis, 1 or 2 for decoy. If biasing 2 bits of overhead: at least 5bits for each state @1GHz = 5Gbps of stream
- **Memory:** these data must be kept in memory until bob tells the click. More latency -> more storage

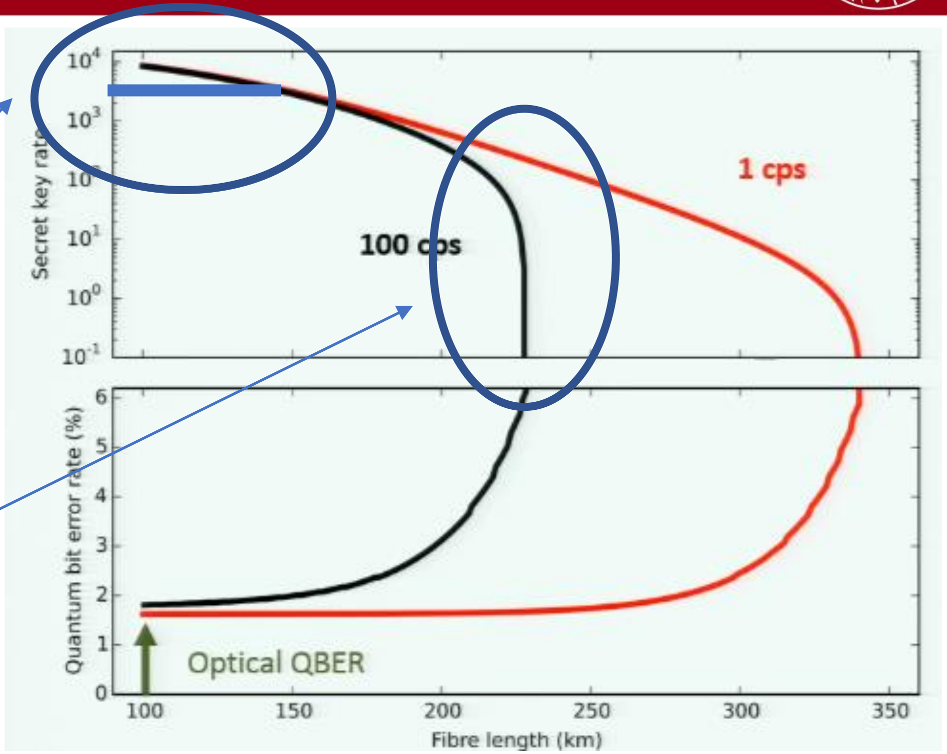
At the receiver side:

- SPAD: saturation at 100khz if not RF gated
- 100 Mbps if RF gated
- SNSPD can go higher
- TimeTagger saturation: 300Mtags/s
- Typical ER/PA saturates at 10Mbps, more need to offload

SKR and detectors

Let’s look at the typical SKR and QBER graph as function of losses

- At low losses SKR limited by QBER and max count rate
- Saturation effect either due to the detector/tagging on post-processing
- At intermediate loss, we have linear scaling with loss
- At high loss sharp knee! Depends a lot on dark count and errors! Why?



The signal: $S \approx \eta f_{max} \approx \frac{\eta}{\Delta t}$

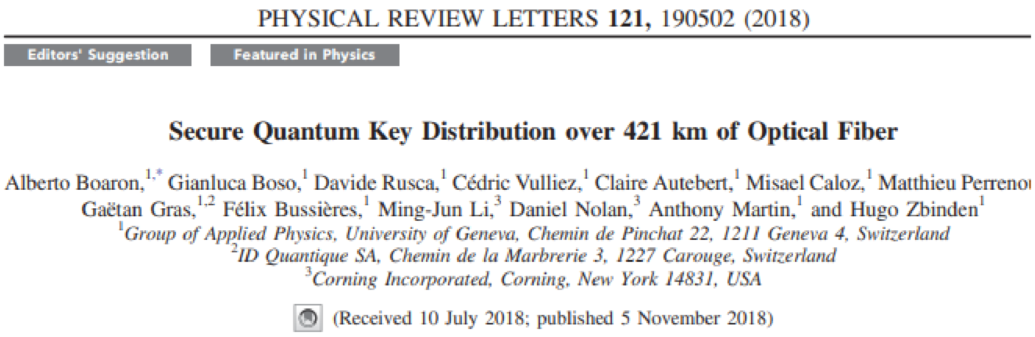
Noise: $N \approx dcr\ \Delta t$

SNR = $\approx \eta\ dcr$

Main limitation to the max distance is given by the errors and dark count of the detector!

SNSPD used for almost all long range demo!

Long range time-bin QKD



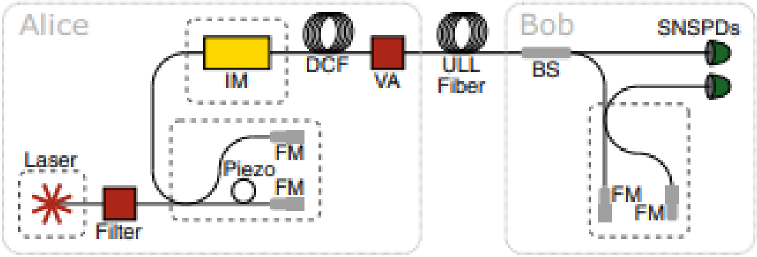
PHYSICAL REVIEW LETTERS **121,** 190502 (2018)

Editors' Suggestion Featured in Physics

Secure Quantum Key Distribution over 421 km of Optical Fiber

Alberto Boaron,[1,*] Gianluca Boso,[1] Davide Rusca,[1] Cédric Vulliez,[1] Claire Autebert,[1] Misael Caloz,[1] Matthieu Perrenou
Gaëtan Gras,[1,2] Félix Bussières,[1] Ming-Jun Li,[3] Daniel Nolan,[3] Anthony Martin,[1] and Hugo Zbinden[1]
[1]*Group of Applied Physics, University of Geneva, Chemin de Pinchat 22, 1211 Geneva 4, Switzerland*
[2]*ID Quantique SA, Chemin de la Marbrerie 3, 1227 Carouge, Switzerland*
[3]*Corning Incorporated, Corning, New York 14831, USA*

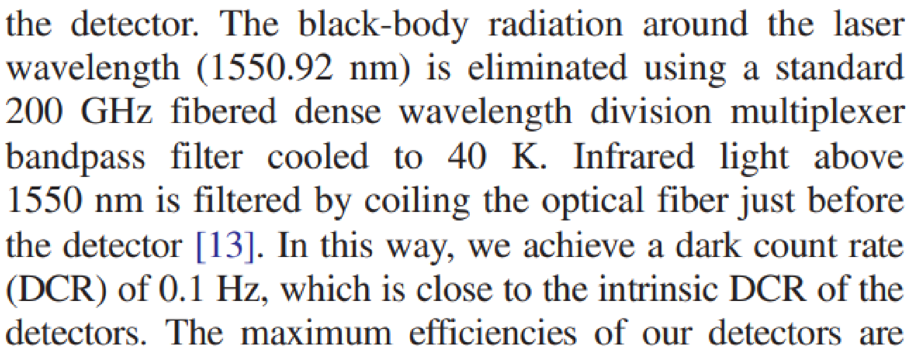
(Received 10 July 2018; published 5 November 2018)



Before the experimental implementations of Twin-Field QKD this was the longest QKD experiment that was demonstrated. Even longer than MDI-QKD (404km)

What is the key point to acheive such long distance ove the fiber?

- The experimental setup was simple and lead to low but not exceptionally low QBER
- High repetition rate helped to get higher SKR but not the distance
- Detection efficiency? Only 40-60% with SNSPD: nice but not ground breaking
- **0,1Hz of DCR and 40ps jitter**



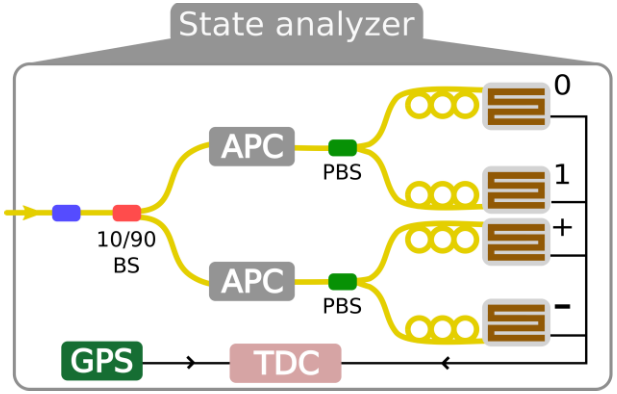
the detector. The black-body radiation around the laser wavelength (1550.92 nm) is eliminated using a standard 200 GHz fibered dense wavelength division multiplexer bandpass filter cooled to 40 K. Infrared light above 1550 nm is filtered by coiling the optical fiber just before the detector [13]. In this way, we achieve a dark count rate (DCR) of 0.1 Hz, which is close to the intrinsic DCR of the detectors. The maximum efficiencies of our detectors are

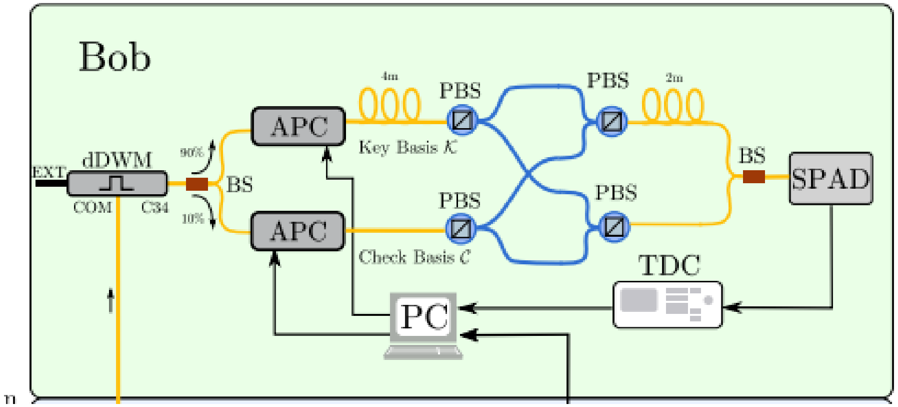
Polarization receivers

Polarization receivers

Typical solution employs a

- BS for a passive choice of the basis,
- two Automatic polarization controller to compensate for the drift introduced by SMF fiber
- Two PBS for the polarization measurement aligned one on the Key and one on the check basis using the APC
- Four Single Photon Detectors for the detection

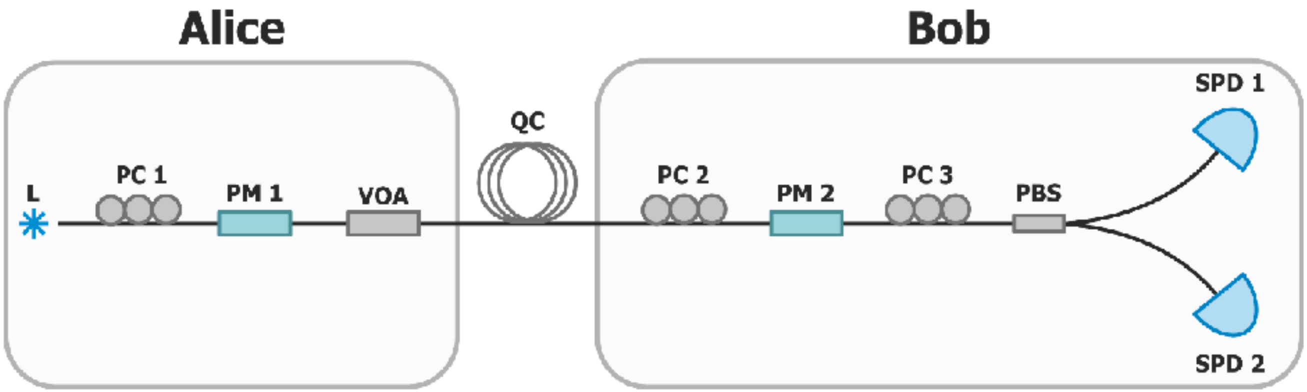




To reduce the number of detectors is possible to perform polarization and time multiplexing at the expense of additional 3db of losses and a factor 4 on the max countrate

Active Polarization receivers

Another option is to use an active receiver where the selection of the basis is performed in real time using a polarization modulator at the receiver side



This configuration allows:

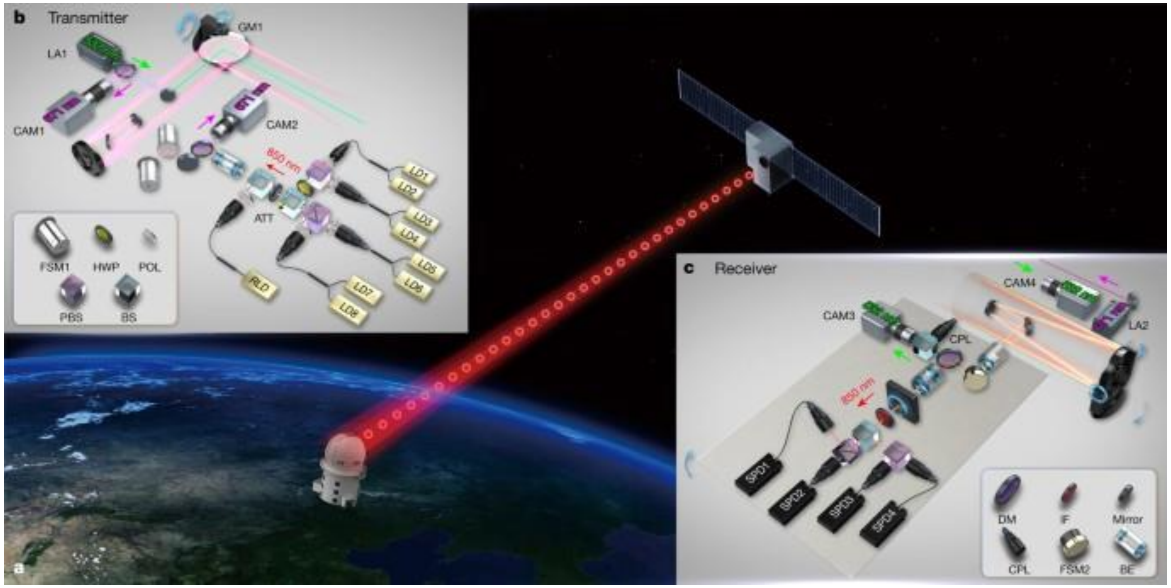
- Reduce the number of detector to 2 without penalty loss from multiplexing

However:

- More losses introduced by the polarization modulator
- Require active measurement -> randomness
- Requires better synchronization at the receiver side

Polarization and free-space/ satellite links

Polarization is mostly used in free-space and satellite links



- Air doesn’t have a significant birefringence, so polarization is preserved
- Due to the Doppler effect satellites add an additional phase to the signal. Need to compensate in the case of time-bin QKD

All free-space transmitter and receivers can potentially be alignment-free after first calibration
For satellite still need to compensate for the rotation of the satellite

Thank you for the attention!

marco.avesani@unipd.it

ThinkQUANTUM

UNIVERSITÀ DEGLI STUDI DI PADOVA