3
Integration within Classical Networks and the Decoy State Implementation

Both experiments explained here were performed during the author's stay with Anders Karlsson's group at KTH between July 2006 and December 2007. They were both based on single-photon sources from spontaneous parametric down-conversion processes in Periodically Poled Lithium Niobate (PPLN) crystals. The first one uses an entangled source of photon-pairs owned by Alice, with one photon detected locally, and the other one transmitted through 27 km of single-mode fiber to Bob. The other key feature of this experiment was that the synchronization classical channel was implemented in the same fiber as the single photons with a channel separation of 0.8 nm. The other experiment employed a heralded single photon source in a QKD experiment using phase coding and the decoy state modification. It was the first experiment to use a sub-poissonian single-photon source with the decoy state protocol.

3.1. Narrowband entangled photon pair source used in a DWDM environment

A practical feature of quantum communication is that we do not need anything other than common commercial optical fibers to use as the quantum channel between Alice and Bob. This is a major advantage to deploy quantum communications in commercial environments since we can use the fibers already installed between two different locations. In order to optimize the use of available resources, classical optical systems typically employ Wavelength Division Multiplexing (WDM) such that each channel (centered each at, λ_1, λ_2,… λ_n) occupies a finite bandwidth. Many modern systems work in a DWDM environment (Dense Wavelength Division Multiplexing) with a channel spacing of 0.8 nm at 1550 nm. It is a quite common practice for the operator who owns the fiber to rent just a single wavelength channel, if the renter desires, such that maximum usage is obtained. Modern filters based on fiber Bragg gratings (FBGs)

or array waveguide gratings (AWGs) ensure that each channel does not interfere with the other. Care must still be taken with non-linear effects happening in the fiber based on the $\chi^{(3)}$ non-linearity, such as four-wave mixing (FWM) and Cross-phase modulation (XPM) [77].

It is therefore, of practical interest, to be able to send quantum signals alongside classical channels inside an optical fiber, since it is more feasible in a commercial sense, to use an optical fiber populated with live traffic, than to require a dark fiber for a quantum communication session. There is another reason to share the quantum communication with classical signals in the same fiber, as both Alice and Bob need to be synchronized. As mentioned in the end of chapter II each qubit sent needs to have a time stamp, and for this matter, the clock signal generated by Alice has to be sent to Bob. In addition to that, the clock signal is normally used to gate the InGaAs SPAD operating in Geiger mode (as it is usually the case for 1550 nm quantum communications). One other reason to multiplex classical and quantum channels in the same fiber would be to implement active polarization control [78]. In this case two channels are required to be used as feedback for the control system. We shall return to this point in Chapter 5.

The source is an improved version of previous efforts by the KTH group on this subject [79,80]. It is a polarization-entangled source of photon pairs, employing two PPLN crystals in an H-V configuration [41], each one being 50 mm long [81]. The motivation for the use of long crystals is to obtain a higher photon pair generation rate, which is proportional to $\sqrt{L}$, and a narrow emission bandwidth, proportional to 1/*L*, where *L* is the crystal's length [82]. To the best of our knowledge this was the first time such long crystals were used in this configuration.

The source is depicted in Fig. 13. We employ a continuous-wave Nd:YAG DPSS (diode pumped solid state) laser, emitting at the wavelength of 532 nm. This laser has an internal laser diode at 808 nm used to pump a Nd:YAG crystal, which generates 1064 nm light, then passing through a non-linear crystal (KTP typically) and gets frequency doubled to 532 nm through second-harmonic generation. The laser beam output goes through a BG39 short-pass filter, to eliminate any residual emission at 808 nm from the diode laser pumping the Nd:YAG crystal, which would be catastrophic to this experiment, as the crystals

are quasi-phase matched for the conversion $532 \rightarrow 809 + 1555\,\text{nm}$. Any photon generated from the pump at 808 nm could be successfully detected degrading the correlation between photon pairs. After the filter we use a half-wave plate (HWP) to rotate the linear polarization of the laser beam.

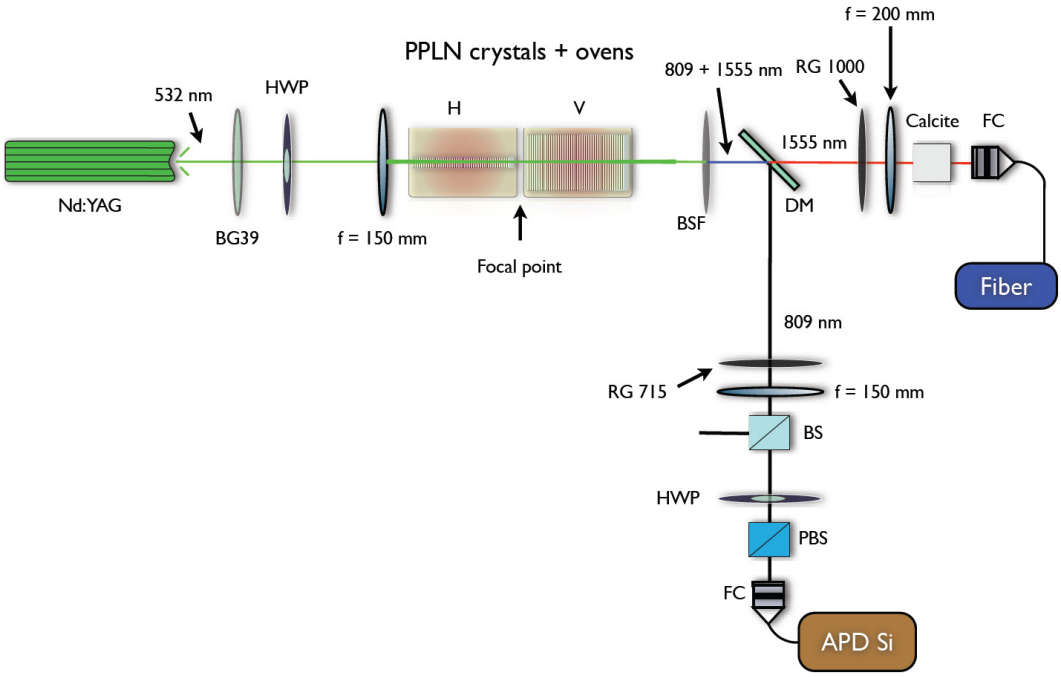

Figure 13 - Entangled single-photon pair source used in the DWDM experiment. HWP: Half-wave plate; BSF: Band-stop filter; DM: Dichroic mirror; BS: Beamsplitter; PBS: Polarizing beamsplitter; FC: Fiber coupler.

The light is rotated to 45º to generate equal probability of conversion in each crystal (since one crystal axis of conversion is oriented in the H direction, and the other in the V direction), and passes through an achromatic doublet lens (focal length = 150 mm) to focus the pump in the middle of both crystals. The crystals generate collinear type-I down-converted light, giving the advantage of better coupling to optical fibers than the cone-like emission in some type-II sources [35]. After the crystals a band-stop filter (BSF) is inserted to remove the pump photons. A dichroic mirror (DM) is used to split the down-converted wavelengths, so that each one may be properly coupled to single-mode fibers. The 809 nm photons are detected by Si APDs (Perkin-Elmer) with 60 % quantum efficiency, operating in passive (free-running) mode. The 1555 nm photons are transmitted via 27 km of SMF-28 (Standard) single-mode telecom fiber to Bob. A home-made InGaAs SPAD module (using an avalanche diode from Epitaxx) with

18\% quantum efficiency working in Geiger mode, is gated by a detection occurring in Alice's Si APD.

The quantum state generated by the source is [81]:

$$|\phi\rangle = \frac{1}{\sqrt{2}}\left(|V(\omega_s)\rangle|V(\omega_i)\rangle + e^{i\varphi}|H(\omega_s)\rangle|H(\omega_i)\rangle\right) \quad (3.1)$$

and $\omega_i + \omega_s = \omega_p$ must be satisfied. ω_p, ω_i and are the frequencies of the pump, idler and signal respectively, and φ is the total phase difference between two polarization components.

The 809 nm photons are locally analyzed by Alice using a passive beamsplitter, to perform the basis choice, and a combination of polarizing beam splitters. The entire analyzing setup is not indicated in Fig. 13, but one extra PBS is missing in the 809 nm arm, which would be connected to the other output of the BS. Also one more half-wave plate is needed on the other arm to convert the D/A (+45º/-45º) basis back to H/V. Four detectors are also needed, two at each PBS. We analyze the state manually rotating the half-wave plate just before the PBS in the idler arm, as indicated in the figure. The down-converted wavelengths can be slightly tuned by changing the temperature of the ovens containing the crystals.

After the down-converted photons are split by DM, they need to be focused into single-mode optical fibers. Because of the input focusing length, the beams are diverging at the output of the crystal and need to be collimated before going through all other components. Because of the different divergence of the beams, different lenses were used, (f_s = 200 mm and f_i = 150 mm), so that each collimated beam gets coupled with a focusing angle matching the numerical aperture of the fibers. In order to remove any residual pump photons that did not get blocked by the BSF filter, we use additional filters in each arm (RG 715 for the idler and RG 1000 for the signal). As mentioned before the 809 nm photon goes through a BS, then a HWP-PBS combination to analyze the state. The photon is finally coupled to a single-mode fiber through FC (containing a short focal length aspheric lens, a fiber holder and a multi-axis translation stage).

A block of calcite is placed on the 1555 nm arm, to compensate the chromatic dispersion generated in the crystals from the fact that the generated wavelengths are so different. In the second crystal V(809) and V(1555) photons

are generated and will separate in time. In the first crystal H(809) and H(1555) photons are emitted, which go through the second crystal generating further dispersion. The net result is that the delay between H(809) and H(1555) is 11 ps larger than the one between V(809) and V(1555) [81]. We use the calcite then, to slow down V(1555) with respect to H(1555), so that the delay between V(1555) and H(1555) with respect to their corresponding idlers is the same. The time of 11 ps is comparable to the calculated 16 ps coherence time of the down-converted photons, which leads to a 75\% visibility decrease in the D/A basis compared to the H/V basis [81]. The piece of calcite gives a 15 ps group delay difference between H and V components, therefore we use a 3-meter long piece of polarization maintaining fiber (PMF), giving a -4 ps group delay difference (slow axis of PMF is aligned to fast axis of calcite). The PMF also allowed us to fine tune the phase difference φ between the two polarization components, by applying a local mechanical strain to the fiber. The PMF is not shown in Fig. 13 for the sake of clarity.

One issue that was discovered about the source employing long crystals is the temperature instabilities between the two ovens. This causes drifts of φ as a function of time due to refractive index changes. These drifts are proportional to the crystal length, and therefore we have severe constraints in that respect since we are using long crystals. It was calculated that a temperature drift of 0.1ºC results in a phase shift between signal and idler polarizations of the order of π, destroying the correlations in the diagonal basis. Our temperature control system, along with isolation of the two crystals inside a transparent box to stop airflow in the room, was just enough to keep the system stable to perform the measurements (several minutes). In order to improve the stability of the source, it would be necessary to replace it by a single-crystal setup [83,84].

In Fig. 14 the entire experimental setup is shown. The signal photon (809 nm) is coupled into a single-mode fiber and detected by a passive-gated Si based APD (Perkin Elmer SPCM AQR-14). Upon successful detection, the Si APD outputs a short electrical pulse (approximately 30 ns wide, 3V amplitude) that goes through a delay generator (DG), which is also used to shorten the pulse width to 10 ns, and then is used to modulate a DFB (distributed feedback laser) with an EA (electro-absorption) modulator built-in (15 dB extinction ratio and 2.5 GHz bandwidth). Each incoming electrical pulse generates an optical one (trigger

signal) with 10 ns width at 1555.75 nm (the laser center wavelength). A circulator (C) and fiber Bragg grating (FBG) centered at the laser wavelength is used to provide additional filtering to remove amplified spontaneous emission (ASE) from the laser. We did not have the FBG installed in the beginning as we only found out that the filtering provided by the wavelength division multiplexers was insufficient when the complete setup was running. In order to relax the filtering requirements we shifted the trigger pulse in time by 50 ns using the delay generator. The signal passes through a single WDM filter module (working as a band-pass filter with 0.5 nm full width-at-half maximum - FWHM, and 0.2 nm flat-top bandwidths), and is then multiplexed at another WDM module with the 1555 nm photon coming from the source (already coupled to single-mode fiber). The 1555 nm photon goes through a 100 m long optical delay consisting of a single-mode fiber cable. This delay is the fiber cable linking the two labs (although located next to each other) where Alice and Bob were located.

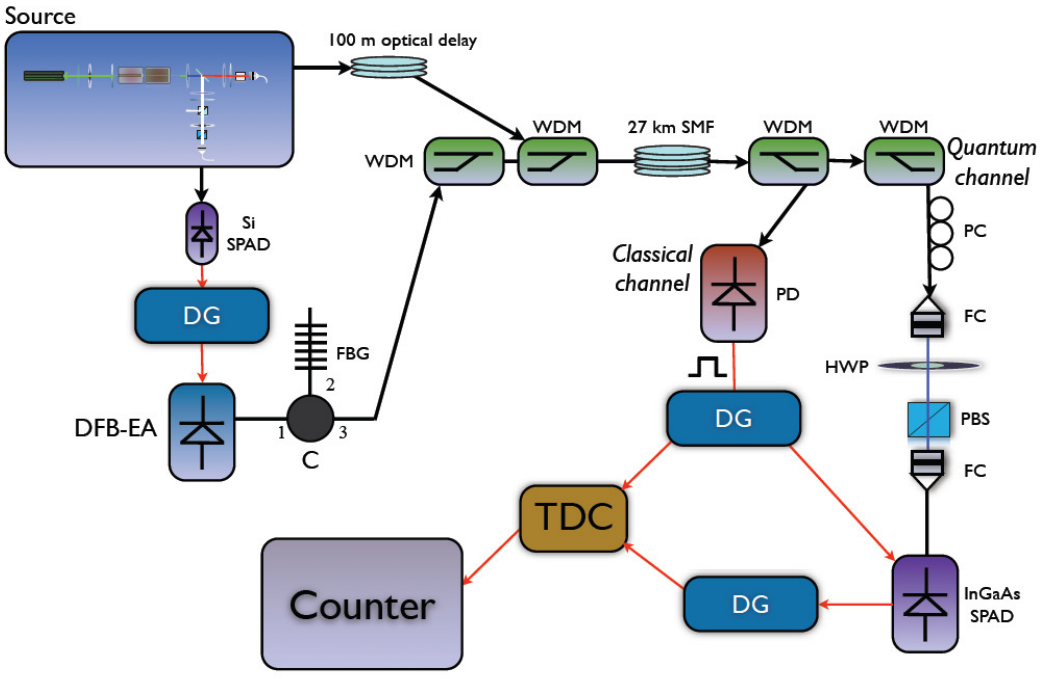

Figure 14 - Complete experimental setup. SPAD: Single photon avalanche detector; DG: Delay generator; DFB-EA: Distributed feedback laser with electro-absorption modulator; FBG: Fiber Bragg grating; WDM: Wavelength division multiplexer; SMF: Single-mode fiber; PC: Polarization controller; PD: Photo-diode; TDC: Time-discriminator circuit. Black lines represent optical fibers, red lines account for electrical connections, and the blue one is free-space.

Both the quantum bit, and the classical pulse are transmitted through 27 km of single-mode fiber, and go through another pair of WDMs working as demultiplexers this time. The classical pulse is reflected in the first WDM, while the quantum signal goes through the other WDM for extra filtering. The classical pulse is detected by a home-made photo-diode (PD, bandwidth of 1 GHz), and its output pulse is connected to another channel of our DG. The 1555 nm photon goes through a manual polarization controller (PC), and a fiber coupler with a collimator before passing a half-wave plate, a PBS and back to fiber again through another coupler. This is done so that the single-photon polarization can be analyzed. The polarization controller is used to adjust the incoming polarization state so that it is linear before going through the HWP. The single photon is then connected to the InGaAs SPAD, which is triggered by one of the outputs of the DG conditioned by the classical trigger pulse. Finally the output of the InGaAs detector passes another channel of the DG, and is connected to one of the inputs of a time-discriminator circuit (TDC) we built to artificially narrow down the gate window. The TDC essentially performs the AND logical operation, with the output of the InGaAs APD and the output of the delayed version of the the trigger pulse (as shown in Fig. 14). Since in a SPDC source, the signal and idler are strongly correlated in time, we can be certain when we should open the detection window (compare this with a weak coherent pulsed source, where the single photon can be anywhere within the attenuated pulse). What we do is to use an AND operation with both pulses, with a smaller overlap between them than the 2.5 ns minimum gate window of the InGaAs APD, through the proper adjustment of the DGs. The price to pay is the loss of some photons (around 20 % for an effective gate window of 1.5 ns), however we simply increased the pump power to compensate. We saw a benefit of a few % gain in all visibility measurements in coincidence counts between signal and idler when using the TDC.

Initially we perform a measurement with only one crystal pumped (although the entire source was aligned, e.g. the focal point of the pump beam in between the crystals), and connected the InGaAs SPAD to detect the 1555 nm photons directly after the fiber coupler at Alice's side. The maximum rate of detection of photon pairs with only the V crystal pumped at a power of approximately 3 mW is $R_c = 25 \times 10^3\ s^{-1}$, with the single count rate at 809 nm $R_s = 0.8 \times 10^6\ s^{-1}$, yielding a conditional detection probability R_c / R_s of around 3 %.

Taking into account the quantum efficiency of the InGaAs SPAD (18 %), we have a corrected probability of detection of 16 %, with no WDM filters present. We measure the accidental (uncorrelated) count rate by triggering the InGaAs SPAD with an external clock at the same single frequency, and we obtained R_a = 0.9 x 10^3 s^{-1}, giving a raw visibility of $V_v = (R_c - R_a) / (R_c+R_a)\$ = 93 %. The spectrum at 1555 nm of the down-converted photons is obtained using an optical spectrum analyzer in place of the InGaAs detector, employing a long integration time and pumping the crystal with maximum power (Fig. 15).

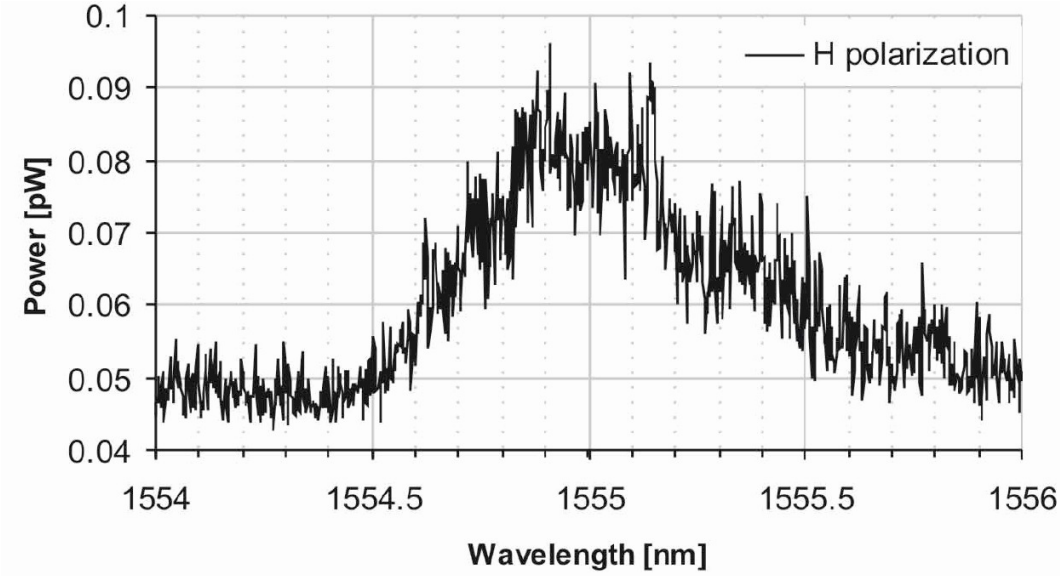

Figure 15 - Spectrum for the 1555 nm down-converted photons, obtained for horizontal polarization without conditional gating at 809 nm. The FWHM is approximately 0.8 nm. Background is the noise level from the optical spectrum analyzer.

For the next step, we pump both crystals (rotating the pump's polarization so that both crystals generate down-converted photons) with the entire setup connected and we measure the visibility curves by using the 809 nm photons as triggers and detecting the 1555 nm ones as a function of Bob's HWP angle with the 100 m fiber cable in place of the optical link (Fig. 16). Synchronization of the system is done by means of an electrical coaxial cable, and a delay generator. The incident pump power on the crystals was of about 4 mW, single count rate of 1.1 x 10^6 s^{-1} at 809 nm and only one WDM filter was used. The coincidence rate R_c dropped by a factor of about three, due to losses in the WDM, and the insertion loss in the free-space polarization analyzer at Bob's side. Measured raw visibilities for each of the four possible polarization states of the signal (809 nm) were V_H =

94 %, V_V = 90 %, V_D = 87 % and V_A = 89 %, for H, V, D and A polarizations respectively. The average predicted QBER from the four visibility curves is 5 %.

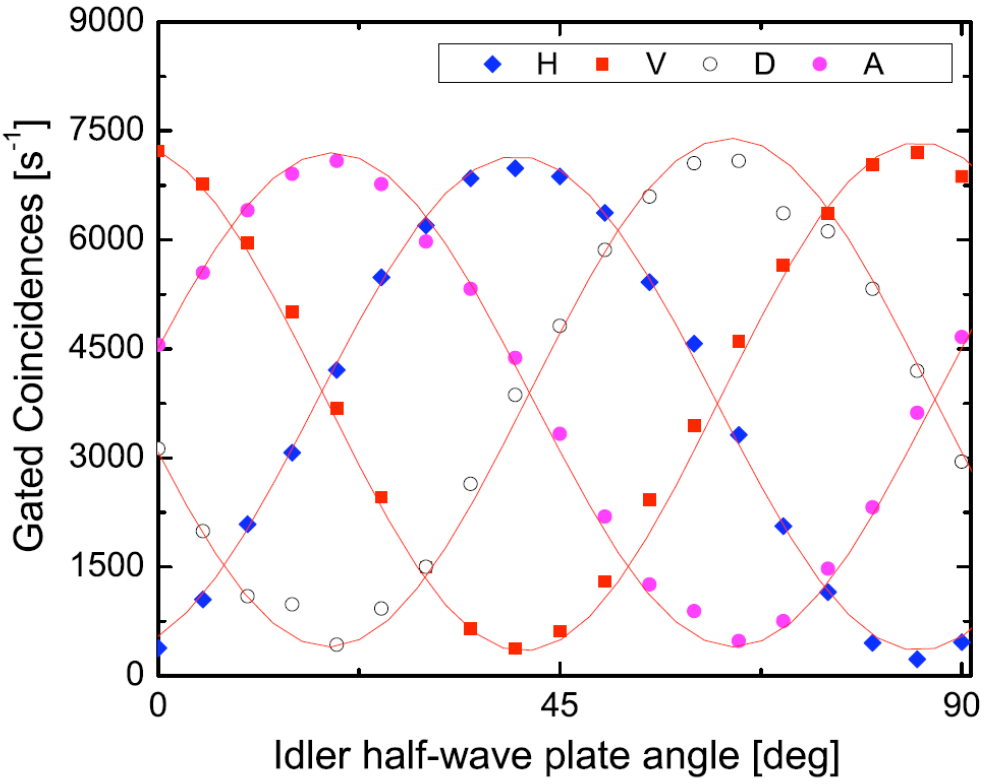

Figure 16 - Visibility curves using coincidence counts as a function of the idler half-wave plate setting for each of the four polarization states of the signal photons (H, V, D and A). Curves show a best fit.

The final part of the experiment is to perform the same visibility measurements with the entire setup connected as in Fig. 14, including the 27 km of SMF, the four WDM filters and the trigger pulses (at 1555.75 nm) sent in the fiber together with the single-photons at 1555 nm. The same incident pump power is used as in the previous part, therefore a single count rate of 1.1 x 10^6 s^{-1} is kept at 809 nm. The coincidence count rate dropped to 1.1 x 10^3 s^{-1} due to the extra attenuation provided by the 27 km fiber link (6 dB), and insertion losses from the other WDMs (3 dB). The raw visibilities for this case decreased to V_H = 85 %, V_V = 85 %, V_D = 83 % and V_A = 85 %. This decrease is due to the losses and trigger channel leakage which we could not fully remove. In hindsight, one of the causes of noise in this experiment could have been Raman spontaneous scattering, which is discussed in the next chapter. The estimated QBER from these curves is around

8\%, averaged over all four polarization states. The polarization state of the idler photons was stable enough for a few minutes, so that the visibility curves could be obtained.

It was shown in this experiment that distribution of single-photons in a quantum network environment (with 0.8 nm channel spacing) is possible, while sending the trigger signal in the same fiber. At the time this work was published, there was only one experiment using the same channel spacing [85]. We have successfully performed the experiment with a narrowband SPDC source, which is a benefit for compatibility with the narrow channels of classical optical networks, and is less sensitive to the effects of chromatic dispersion inside the optical fiber.

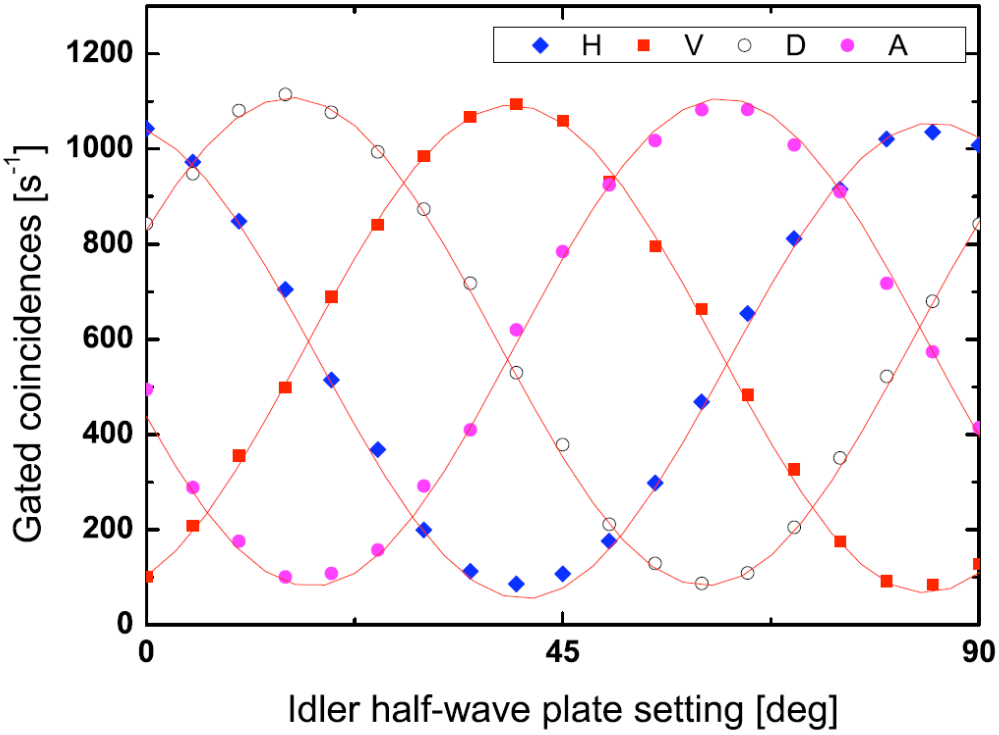

Figure 17 - Visibility curves after 27 km of single-mode fiber using coincidence counts as a function of the idler half-wave plate setting for each of the four polarization states of the signal (H, V, D and A). Curves show a best fit.

3.2. Experimental QKD with a Heralded Single-Photon Source and the Decoy State Modification

Even though there have been extensive proofs of security for QKD [86,87,88], there is one type of attack Eve can perform which takes advantage of realistic photon sources called the photon number splitting (PNS) attack [89-90].

This type of attack can succeed against sources that emit multi-photon states, and for this reason only QKD schemes using perfect single-photon sources are secure against this type of attack. All current photon sources employed in quantum communications are approximations to the ideal single-photon source, with the attenuated laser generating weak coherent states (WCS) being the worst. Depending on the average photon number per pulse chosen (typically 0.1), WCS sources may be used for secure QKD, but there is a large vacuum component (empty pulses, around 90 % of the total) which severely limits the transmission rate. If the average photon number is higher, then the multi-photon component (pulses containing two photons or more) increases considerably, and the PNS attack becomes possible. In fact for secure QKD, the following condition must apply [89,91].

$$y > p_{multi} \tag{3.1}$$

We shall now describe the idea behind the PNS attack: Eve monitors the quantum communication channel between Alice and Bob, and performs a quantum non-demolition measurement (QND) [92] to find out how many photons are in each pulse. Remember that Eve has access to technology that is not even developed yet, as long as it is physically feasible. Every instant a single-photon pulse is detected by Eve, she simply blocks it and all the times a multi-photon pulse is detected, she splits it keeping one photon for herself and forwarding the other to Bob. Eve stores her photon in a quantum memory (this was far-fetched technology when the PNS attack was first mentioned, but it is getting more and more practical [93,94]) and awaits until the basis choices are revealed by Alice and Bob over the public channel. Then she measures the photons with full certainty, obtaining full information about the key. If this is all Eve does, Bob will clearly realize something is wrong, since all single-photon pulses are not reaching him (we are assuming he does not have photon-number resolving detectors, but he realizes that less pulses are being detected). The PNS attack becomes more difficult to detect when the source has a large multi-photon component, in other words, a low quality single-photon source is being used by Alice. Eve is obviously smarter than that. In order to disguise her presence, she replaces the part of the communication channel after the point of her interception by a lossless channel (for example a perfect teleportation apparatus). Eve's presence can be

more easily masked if the loss and multi-photon component are higher. These two conditions can be summarized by Eq. (3.1), and the PNS attack is summarized in Fig. 18.

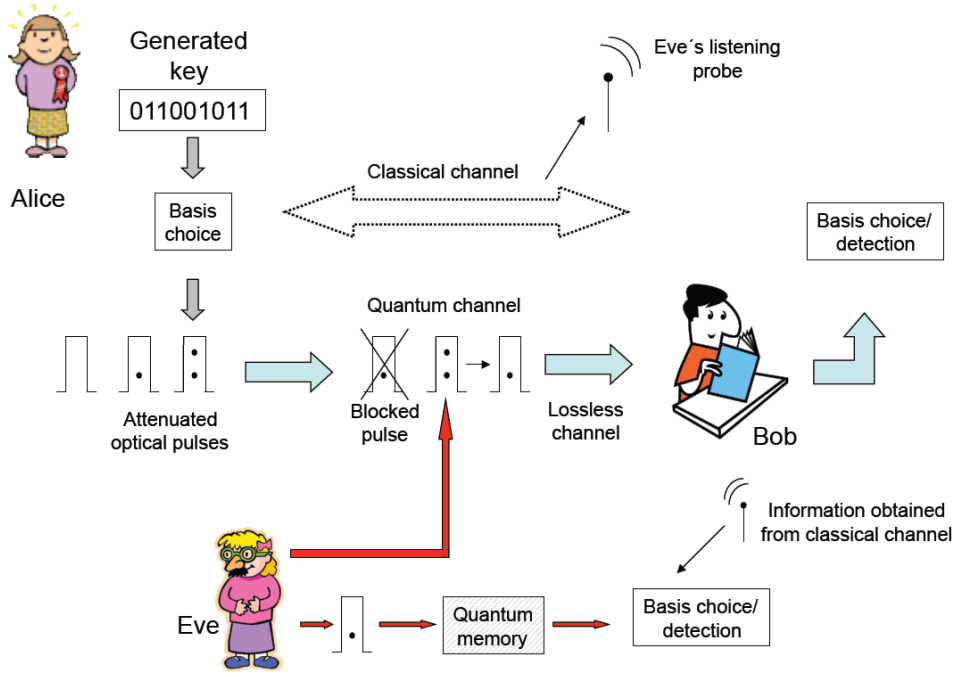

Figure 18 - PNS attack scheme. Adapted from [72].

The PNS attack defines what is the actual secure transmitted distance, even if the reachable distance is much higher. For example, using the experimental data from [95], Brassard *et al* [89] have shown that the secure transmitted distance was zero, even though the experiment managed to share a key through 30 km, using an average photon number per pulse of 0.2. The large vacuum component of the source used (attenuated pulsed laser) causes difficulties for this type of source, as well as the multi-photon probability. One solution is to use a source based on SPDC processes, since the vacuum component and the multi-photon probabilities are both smaller. Indeed, changing the source used in [95] and using the same data for the optical fiber and detectors used, Brassard *et al* [89] have shown that a secure distance of 68 km could be achieved with a SPDC source.

From the results mentioned above, it seems that sources based on weak coherent states are not secure enough against a technologically superior Eve, and that SPDC-based sources seem to be a solution. However, even today they are much more expensive and complex than an attenuated pulsed laser. Fortunately a

major breakthrough came in 2003 with the idea of decoy states developed by Hwang [91] and later improved [96,97].

The decoy state method is based in the idea that Alice sends multi-photon pulses on purpose to Bob, in order to trick Eve in performing a PNS attack. The key to this method is that Eve cannot predict if a multi-photon pulse was intentionally generated by Alice, or if it is a source imperfection, thus she will perform the PNS attack on all multi-photon pulses. The protocol works as follows: Alice randomly chooses between different intensity levels for each pulse being sent. We shall refer here only to the three-state protocol [96] in which Alice sends vacuum, signal and decoy pulses with 0, μ and μ' average photon numbers respectively, where $\mu' > \mu$\$. She can change which type of pulse she wishes to send by using a variable optical attenuator. Other important parameters are the counting rates (or yield) measured by Bob Y_0, Y_μ and $Y_{\mu'}$. After all the pulses are sent out, Bob informs through the public channel which pulses caused clicks on the detectors, and which did not. Alice knows which type of pulse was sent each time, and from the results informed by Bob, she can deduce the counting rates for each type of pulse.

Let us now look at it from another perspective. If Eve blocks all the single-photon pulses, the transmittance of multi-photon pulses should be abnormally high when compared to the single-photon ones. In other words, the normalized counting rates (over the number of pulses) for multi-photon pulses will be higher than single-photon pulses. Alice and Bob can calculate a lower bound for the single-photon counting rate of single-photon states and an upper bound of the quantum bit error rate of single-photon states. They can then discover if Eve is attempting the PNS attack. The decoy state idea has dramatically improved the secure transmission distance [97]. This is just the general idea of the decoy state method, for a more rigorous discussion please see [91,96,97]. For experimental realizations please see [59,98].

Decoy states represent a major improvement for the security of systems using attenuated pulsed lasers as the single-photon source. But what about a source based on SPDC? A heralded single-photon source (HSPS) is in principle a perfect single-photon source, since for every detected signal photon, there is a corresponding idler photon. A practical HSPS, however, will have losses, and

those will create empty pulses. Multi-photon pulses are also created due to high intensity pump powers though this probability is much lower than sources with weak coherent states. Nevertheless it was shown that the decoy state method can improve the secure transmitted distance of an HSPS too [99,100,101]. This experiment then combines an HSPS with the decoy state method performing a QKD session over an optical fiber link [34].

The experiment was done in Stockholm as a collaboration between KTH and the University of Science and Technology of China from Hefei, with the group of Guang-Can Guo. The source was assembled at KTH and when it was ready, members from Hefei brought in their phase-coding setup and electronics to perform a QKD session. We shall first describe the HSPS we built for the experiment. Originally a 20 mm long PPLN crystal with a waveguide was used in the HSPS, for the same conversion of $532 \rightarrow 809 + 1555\,\text{nm}$. A great deal of time was spent adapting the oven containing the crystal to the optical setup. After spending some more time aligning the optics, we discovered that the conversion was completely off from the specified. Although the brightness was clearly much superior than the long crystals used in the narrowband source experiment, the the wavelength was not compatible with optical fiber transmission (emission was at around 1200 nm for the idler). We made the quick decision of replacing the waveguide with one of the 50 mm long PPLN crystals used in the previous experiment explained in the previous section, especially since, as mentioned, the entangled source of photon-pairs would move on to a single-crystal configuration.

The scheme for our HSPS is shown in Fig. 19. The pump is a Nd:YAG DPSS laser. The pump beam is focused in the middle of the PPLN crystal using a 150 mm focal length achromatic doublet lens. This focal length was chosen after some attempts based on the focusing conditions of the previous experiment. However, no collimating lens was used to the output down-converted beams, and instead we placed the dichroic mirror (DM), filters and fiber couplers very close to crystal, so that the beams did not diverge too much. The fiber coupler (FC) is composed of a short focal length aspheric lens, a multi-axis translation stage and optical fiber holder. The signal FC was placed at half the distance from the DM when compared to the idler FC, in order to compensate the beam divergences in

the coupling. We also tried using extra collimating lenses but the final results were approximately the same, so we opted for the simpler setup.

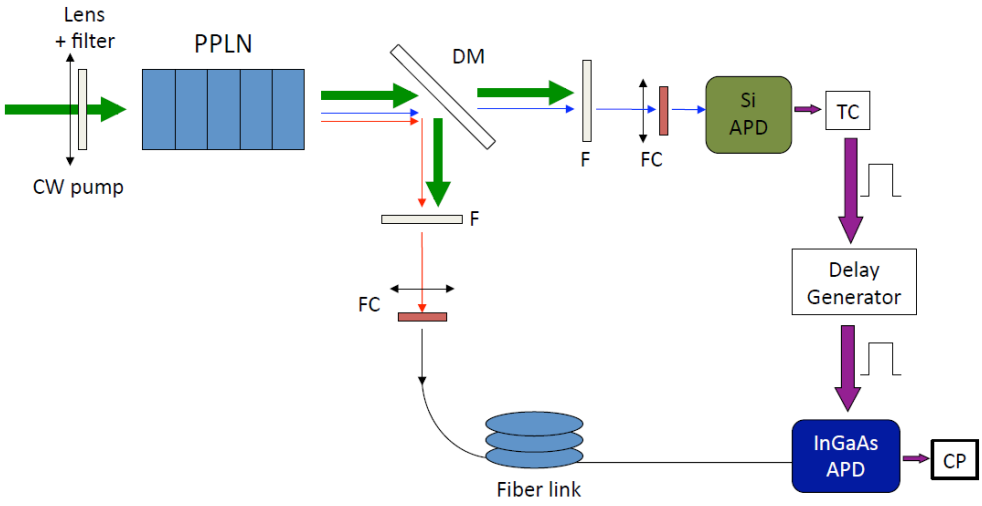

Figure 19 - Heralded single photon source used in the experiment. PPLN: Periodically-poled lithium niobate crystal; DM: Dichroic mirror; F: Filter; FC: Fiber coupler with aspheric lens and multi-axis translation stage; TC: Time chopper; CP: Counter and processing. Green, blue and red arrows represent pump, signal (809 nm) and idler (1555 nm) respectively. A HWP is used to adjust the pump polarization before the crystal (not shown).

After the DM, two bulk filters are used to remove the pump from the signal and idler beams (RG 715 and RG 1000 respectively). Both beams are coupled to single-mode optical fibers before arriving at the Si and InGaAs detectors. The Si APD was the same as the one used in the previous experiment (Perkin Elmer), while the InGaAs APD operating in Geiger mode was changed (IdQuantique id200). It has a quantum efficiency of 7.5 % and 2.5 ns gates were used. After the Si APD we employed a Time Chopper (TC), used to insert a dead time after each detection. It is necessary because in order to change the average idler photon number per detection window we need to change the pump power, and as a consequence the signal photon rate. When we do so, we change the triggering rate in the InGaAs APD, and the dark count probability also changes. Therefore, with a deadtime, the InGaAs triggering rate did not rise as fast as the number of detections by the Si APD, and our set up did not see the difference in the dark count probability when we changed between , μ and μ' . The output of the TC is connected to a delay generator, and finally to the trigger input of the

InGaAs APD. The idler photon, after coupling, will go through the optical fiber until before detection by the InGaAs APD.

The initial step is to characterize the HSPS, and we employed the same method as in [102] described in detail in [103]. We would like to know what type of photon distribution our source emits. When using a CW pump, as long as the coherence time Δt_c of the down-converted photons is shorter than the gate width, a large number of independent down-conversion processes will take place, resulting in a poissonian distribution [103]. One important parameter for the characterization of a single-photon source is the second-order auto-correlation function at zero-time delay [16,103]:

$$g^{(2)}(0) = \frac{2P_{m\geq 2}}{P_{m\geq 1}^2} . \qquad (3.2)$$

If $g^{(2)}(0) = 1$ we have a poissonian source, $g^{(2)}(0) < 1$ it is sub-poissonian and and finally $g^{(2)}(0) > 1$ super-poissonian [16]. $P_{m\geq k}$ is the probability to find at least *k* photons within a gate period, which can be written as:

$$P_{m\geq k} = P^{cor} P_{m\geq k-1}^{acc} + (1 - P^{cor}) P_{m\geq k}^{acc} \qquad (3.3)$$

where P^{cor} is the correlated rate of photon pairs, which is the probability of detecting an idler photon (heralded) given that a signal photon (heralding) has been detected. If there are no losses in the system (perfect coupling and components), then $P^{cor} = 1 \cdot P_{m\geq k}^{acc}$ is the probability that at least *k* accidental photons fall within a gate period, that is, uncorrelated photons. Since the accidental photons are not correlated, the pump is CW and the coherence time of the down-converted light is much smaller than the gate width, the distribution of these photons is poissonian. As we will see, our source fall within these conditions, since the emitted coherence time is around 10 ps, and the gate width is 2.5 ns. Therefore, $P_{m\geq k}^{acc}$ can be written as [102,103]:

$$P_{m\geq k}^{acc} = 1 - \sum_{i=0}^{k-1} \frac{\mu^i}{i!} e^{-\mu}, \qquad (k \geq 2) \qquad (3.4)$$

where μ is the average photon number per gate, $\mu = R_i \cdot \Delta t_{gate}$, R_i is the mean photon number per second, is the gate width of the detector. We denote r_c the coincidence count rate; r_s the Si APD single counting rate; r_i the InGaAs detector single counting rate (using random triggering, whose frequency is R_0); R_0 is the heralding rate which can be different from r_s due to the dead time of the detector / delay generator; η_i (η_s) and d_i (d_s) are the detection efficiency and dark count probability of idler and signal detectors respectively; R_i (R_s) is the photon number per gate present in the fiber before detection.

Using the steps shown in [103] we can write:

$$R_s = \frac{1}{\eta_i \Delta t_{gate}} \ln \frac{R_0 - d_i}{R_0 - r_i} \tag{3.5}$$

$$P^{cor} = 1 - \frac{R_0 - r_c}{R_0 - d_s} e^{\eta_s R_s \Delta t_{gate}} \tag{3.6}$$

All the parameters in Eqs. (3.5) and (3.6) can be measured in the experiment yielding the values of P^{cor} and R_s. Writing expressions for the probability to detect *n* photons, vacuum, the single-photon, and substituting the values of $\$ P^{cor}$ and R_s into those expressions (steps outlined in [103]) we can calculate the photon number distribution of our source as shown in the table below for two different trigger frequencies (or in other words, pump power) after the time chopper, 200 and 650 kHz, corresponding to μ and μ' respectively. The intensity is the average number of photons per detection window and p_0, p_1 and p_2 correspond to the vacuum, single and two-photon probabilities per detection window:

Trigger (kHz)	Intensity	p_0	p_1	p_2	$g^{(2)}(0)$	P^{cor}
200	0.588×10^{-3}	0.727	0.273	1.600×10^{-4}	4.56×10^{-3}	0.273
650	5.532×10^{-3}	0.698	0.300	1.655×10^{-4}	3.53×10^{-2}	0.298

From these results we clearly see that our source exhibits sub-poissonian characteristics $g^{(2)}(0) < 1$ and very low multi-photon probability, showing that we have an improvement when compared to a weak coherent source. A photo of part of the source is shown in Fig. 20:

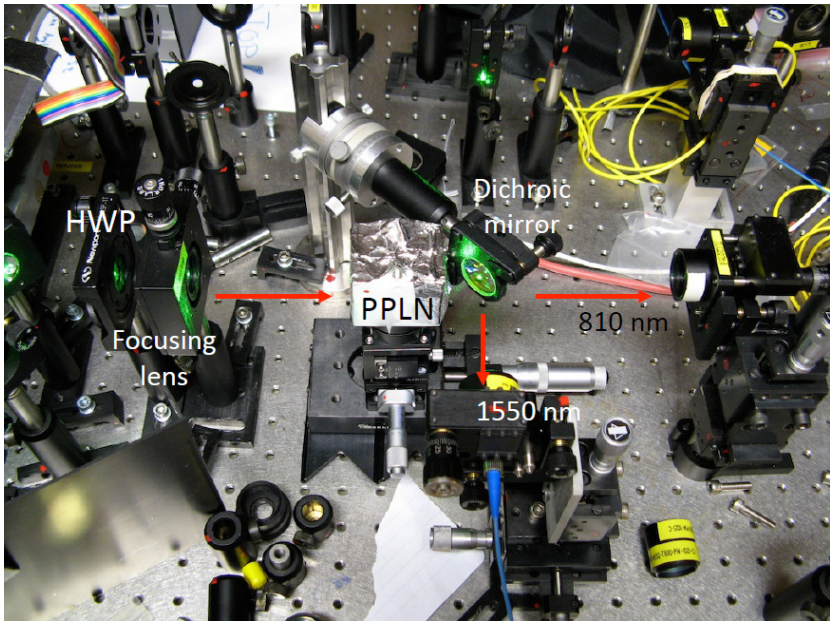

Figure 20 - Picture of part of the source. The pump laser, electronics and detectors are not shown.

Taking the data obtained from the source characterization and using the same method from [99,100,101] and as shown in [34, 103], we plot the key generation rate vs the total losses comparing several different schemes:

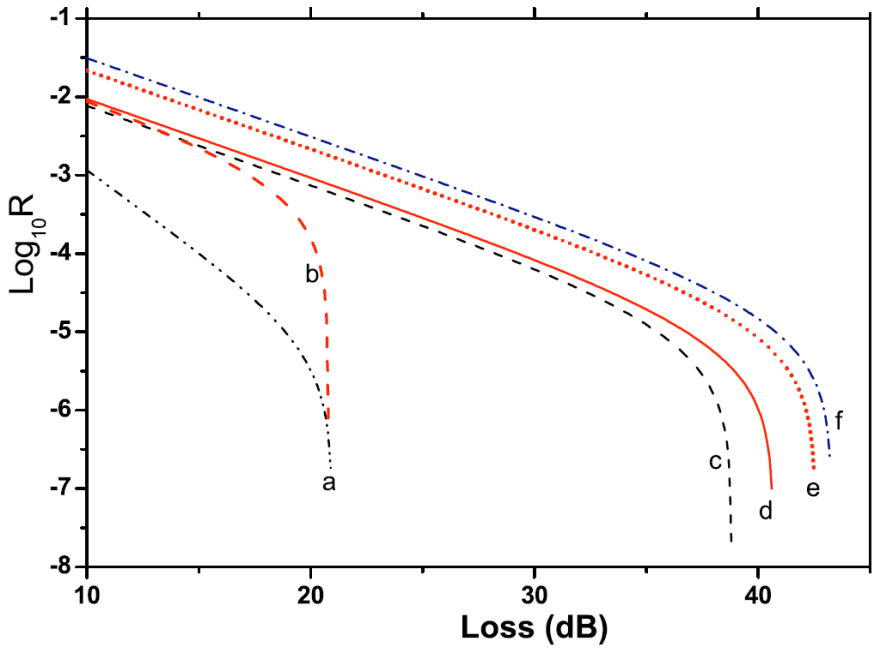

Figure 21 - Numerical simulation for the key generation rate vs total loss for the following schemes: a) WCS source without decoy state; b) HSPS without decoy state; c) WCS with decoy state method (optimal values for used for each point); d) HSPS with decoy state with P^{cor} = 30 %, μ = 5.88 x 10^{-4} and μ' = 5.53 x 10^{-3}, values taken from our source

characterization; e) HSPS with decoy state and with P^{cor} = 70\%, and μ and μ' values as before; f) the ideal single-photon source.

Fig. 21 clearly that shows our scheme outperforms an attenuated pulsed laser source using optimized decoy states. Curve e) shows what could be obtained if an HSPS with P^{cor} = 70\% was used with the same values for μ and μ' as our source. Such an HSPS was recently demonstrated [104] using narrow filters, therefore it is technologically feasible, and its performance comes very close to the ideal single-photon source. Optimizing our source we obtained $P^{cor} = 40\ \%$ in [103]. The entire experimental setup is shown in Fig. 22:

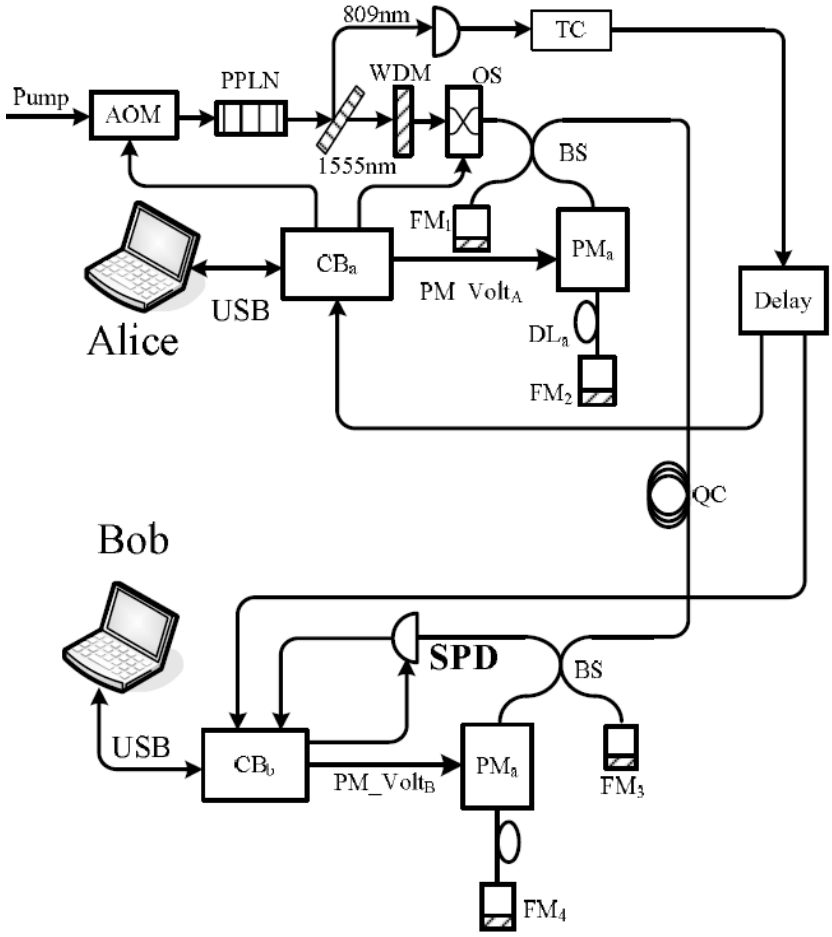

Figure 22 - Complete experimental setup of QKD with an HSPS using the decoy state method. AOM: Acousto-optical modulator; PPLN: Periodic poled lithium niobate; WDM: Wavelength division multiplexer; OS: Optical switch; TC: Time chopper; BS: Beam splitter; PM: Phase modulator; FM: Faraday mirror; CB: Control board; DL: Delay line; SPD Single photon detector.

The QKD phase-coding setup is based on a one-way Faraday-Michelson (F-M) system [105], using four states with one detector scheme, making it immune to time-shift [106] and faked-states [107] attacks, with the disadvantage of losing half of the photons. This scheme is also immune to birefringence changes like the "Plug and play" setup, but it has the advantage of being one-way.

In order to create the decoy states, we could simply place a fiber-pigtailed amplitude modulator after the 1555 nm signal coupling. However, as we will discuss below, our system has too much loss, and the > 3 dB insertion loss in commercial optical amplitude fiber-based modulators for 1550 nm was too much. Therefore we placed an Acousto-optical modulator (AOM) in the pump beam path before the crystal. One problem we would have is how to create the vacuum state in this configuration, because we would lose all triggering signal by fully attenuating the pump. We then inserted a fiber pig-tailed optical switch with 0.6 dB loss to change between μ_0 (vacuum) and μ states, and the AOM changing between μ and μ' states. As mentioned before the electronic time chopper (TC) was necessary to keep the same dark count probability, while changing the pump's power with the AOM to generate μ and μ'.

The F-M system was intended to be used originally with a WCS source, and therefore the attenuation at Alice does not matter as she can simply adjust her attenuator accordingly. For an HSPS *any* attenuation means less photons arriving at Bob. The F-M configuration + HSPS is even more restrictive at that, since the signal passes twice through the phase modulators when compared to a standard phase scheme. Right from the start, loss was one of the most difficult issues with this experiment. That is the reason why we had to minimize losses, the best as possible. Another major issue was the coherence length of the source required to obtain interference in the interferometers. The interferometers were designed to be used with an attenuated pulsed laser, which has a very narrow linewidth. The length mismatch between the two interferometers was too long as we observed visibilities of less than 10 % with the HSPS, which makes any quantum communication session unfeasible. Using a classical broadband light source centered around 1550 nm, connecting the two interferometers in series, measuring the spectrum of such source in an optical spectrum analyzer and observing the fringes generated we estimated the length mismatch to be on the order of 1 cm. Using the spectrum of our HSPS (Fig. 23), we estimated that the required length

mismatch should be in the order of 2-3 mm. Even though the crystal is the same as in the previous experiment, we obtained a brighter source when comparing the optical power from the two spectra (this one and the spectrum of the entangled photon-pair source using two crystals) due to optimized focusing conditions and coupling, to a much simpler configuration of the source, and to less optical components involved.

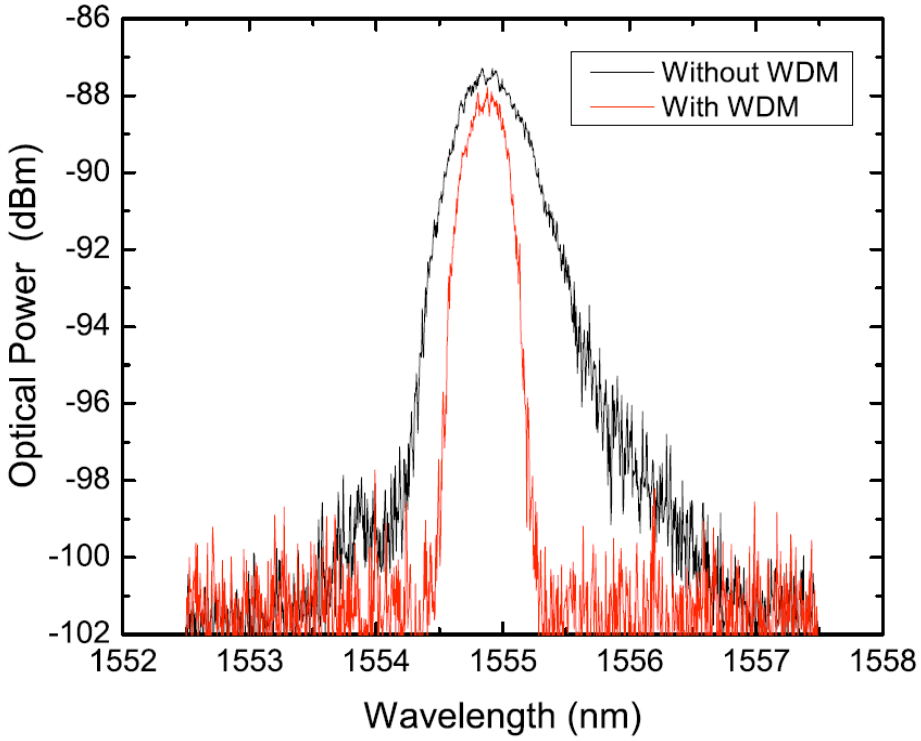

Figure 23 - Spectrum of the down-converted idler photons with (red) and without (black) WDM filter.

In order to adapt the interferometers to our source we decided to open up their thermally insulated boxes, cut one of them, and use a fiber splicer to adjust the lengths. It was a trial-and-error procedure, since we had to get the length adjusted to within less than 2 mm. After we managed to adjust it (we checked with the broadband light source and spectrum analyzer), the visibility curve had improved considerably, but it was not good enough, since high QBERs were obtained even with no fiber. We finally used a WDM filter (from the previous experiment) to narrow down the spectrum of the HSPS as shown in Fig. 23. We had to bear with a total loss of almost 3 dB (insertion loss + narrower spectrum), but it was the only way to get a good visibility (> 95 %) to perform the experiment.

The average photon number per 2.5 ns gate is for each intensity: [μ', μ, μ_0] = [5.532 x 10^{-3}, 0.588 x 10^{-3}, 0.577 x 10^{-5}], and due to an imperfect isolation ratio of the optical switch (20 dB), our vacuum state is a bit higher than just the dark counts. The ratio between the number of states sent for each type was 10:4:1. The interferometers were built inside thermal insulated containers, and they were stable enough for usage for only a few seconds. There was no active temperature controllers built-in. In order to improve the insulation we made a larger box filled with styrofoam pieces and placed both interferometer containers inside. The stability improved to around 1 min, which is clearly not enough for a QKD session, therefore we adopted a scan and transmission mode [105] in which we transmit blocks of key, then stop the transmission, scan the interferometer to measure the visibility adjusting the voltage bias of the phase modulators. This has the negative effect of dropping the overall key transmission rate, but no active control is required.

Alice and Bob are connected by 25 km of standard SMF-28 optical fiber, with a total loss of 5dB. Unlike the previous experiment, we did not send the trigger pulses in the fiber along with the quantum signals. We were so limited in terms of loss, that we would not be able to use the set of 4 DWDM filters. Therefore the synchronization was done using electrical cables and a delay generator to match the times. We estimated the required delay for the fiber. Then we made a quick search around that value until we found the coincidence peak. During a measurement of 200 minutes (the actual key transmission time is 70 minutes, without the scan time), the total QBER for μ (μ') was 6.43 % (6.88 %), and we obtained 30.90 x 10^3 sifted key bits out of a total of 84.60 x 10^3 coincidence counts after a total loss of 36 dB (fiber + QKD setup after fiber coupling). Finally, 3.77 \times 10^3 secure key bits can be distilled, which agrees well with the theory, as shown in Fig. 24, using the simulation model described in references [97,99,100].

Our final key rate is lower than most QKD systems due to the high loss present in the optical setup. Many things could be done to decrease the loss, such as replacing the F-M system by a Mach-Zehnder configuration [7], using polarization encoding, using a standard two-detectors scheme and replacing the InGaAs detector by a newer model with higher quantum efficiency and lower dark counts. All in all, we could gain 15 dB which would make our experiment more

reliable for long distance transmission or higher key rates. However as a proof-of-principle experiment we showed that QKD with an HSPS with the decoy-state method is feasible, and offers performance gains over standard decoy-state with a WCS source.

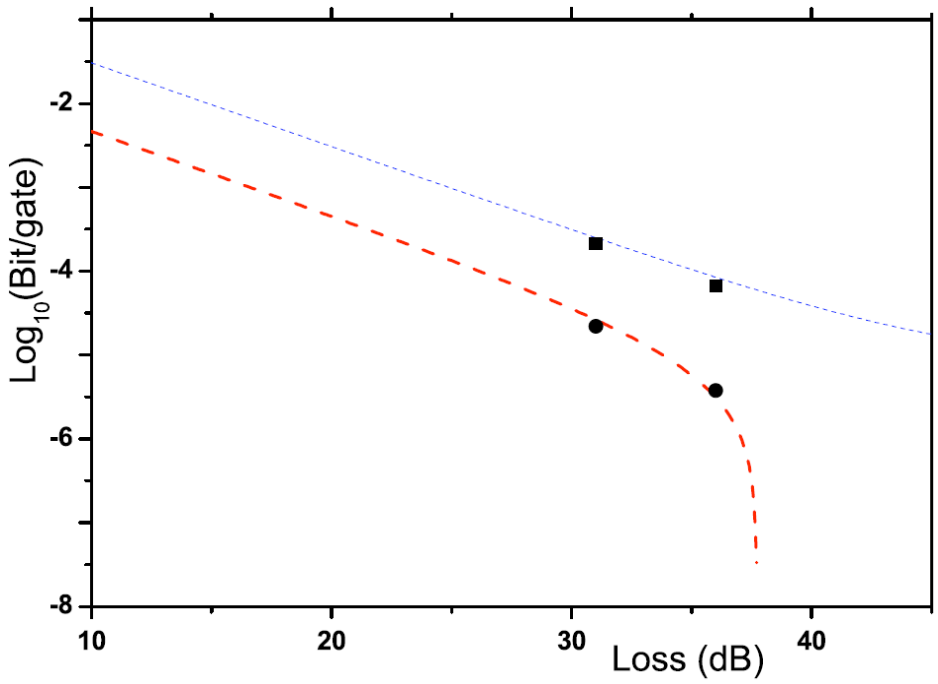

Figure 24 - Theoretical curves for the coincidence count rate (dotted blue line) and final secure key rate (dashed red line). The dots and squares are the experimental results at a total loss of 31 (optical fiber removed) and 36 dB (25 km of spooled SMF-28 fiber connected).