Università degli Studi di Padova
Dipartimento di Fisica e Astronomia
"Galileo Galilei"

Corso di Laurea Magistrale in Fisica

Quantum Memories for Quantum Communication

Laureanda:

Alessia Scriminich

Relatore: Prof. Paolo Villoresi
Correlatore: Prof. Giuseppe Vallone

Anno Accademico 2016/2017

Abstract

Quantum memories are quantum light-matter interfaces able to receive, store and retrieve a quantum state with a fidelity higher than any classical device. They will be an essential element of future Quantum Key Distribution (QKD) networks, where the properties of quantum systems are exploited to achieve information-theoretic unconditional security. In this thesis, I studied the application of Rubidium-vapour room-temperature quantum memories for the storage of polarisation qubits and particularly the possibility of interfering the pulses stored in the memory both at a classical and quantum level. The two-photon interference effect is indeed at the basis of the recently developed Measurement-Device-Independent QKD protocols. Specifically, I set up two twin polarisation qubit sources and interfered their outputs to measure classical beat-note interference and quantum HOM two-photon interference. One of the pulses was then stored in a quantum memory and interfered with the delayed output of the other source. The storage time of the memory was adjusted to compensate for the delay. I also designed and developed a driver for the electro-optic polarisation modulator of the qubit source for a future QKD experiment. The driver is composed of a 4-level high-voltage switch circuit and a FPGA I programmed to act as a digital interface for both sources.

Sommario

Le memorie quantistiche sono interfacce luce-materia in grado di ricevere, memorizzare e riprodurre uno stato quantistico con una "fidelity" più alta di qualsiasi altro dispositivo classico. Saranno un elemento essenziale di future reti di distribuzione di chiave quantistica (QKD), dove le proprietà quantistiche della materia sono struttate per permettere un livello assoluto di sicurezza. In questa tesi, ho studiato l'applicazione delle memorie quantistiche a vapori di rubidio a temperatura ambiente per la memorizzazione di qubit in polarizzazione ed in particolare la possibilità di far interferire gli impulsi immagazzinati sia a livello classico che quantistico. L'interferenza a due fotoni è infatti alla base dei protocolli Measurement-Device-Independent QKD recentemente sviluppati. Nello specifico, ho realizzato due sorgenti di qubit in polarizzazione ed interferito i loro output per misurare interferenza classica e interferenza quantistica a due fotoni. L'output di una delle sorgenti è stato successivamente memorizzato in una memoria ed ho misurato l'interferenza tra un impulso memorizzato ed un impulso ritardato proveniente dall'altra sorgente. Il tempo di memoria può essere regolato per compensare esattamente il ritardo inserito. Ho inoltre progettato e realizzato un driver per il modulatore di polarizzazione elettro-ottico della sorgente di qubit per un futuro esperimento di QKD. Il driver è composto da un circuito di switching a 4 livelli in alta tensione ed un FPGA che ho programmato per fungere da interfaccia digitale per entrambe le sorgenti.

Contents

List of Figures

1 Introduction

The aim of this Chapter is to introduce the background of this work, particularly the ideas behind Quantum Communication and how information can be encoded in quantum states to achieve unconditional security, and the principle of operation of room-temperature Quantum Memories and their application as a building block of future Quantum Networks. Specifically, I will explain the theory behind electromagnetically induced transparency, the effect that enables the operation of the quantum memories studied in this work.

1.1 Quantum Communication

1.1.1 Advantages of Quantum Cryptography

Classical protocols for sharing secure information can be divided into two main approaches: private key cryptography and public key cryptography.

The critical step in private key cryptography is the exchange of a secret encryption key. Provided that the channel is private, a randomly generated key of the same length as the message will ensure that the communication be secure and the encryption can then be performed by simple prococols such as the Vernam cypher or one-time pad. The obvious issue with this type of cryptography is that it may require an extremely long key, and for this reason public key cryptography was developed in the 1970s. The security of this protocol is no longer ensured by the secrecy of the keys, but by the complexity of the encryption algorithm which is based, for instance, on multiplication for the widely employed RSA protocol. In this case, an eavesdropper may try to decrypt the message and extract the key by applying a factorisation or order-finding algorithm. Such algorithms do exist but are classically inefficient and therefore the security of the protocol relies heavily on the limited computational power of a possible eavesdropper.

When tested against a quantum adversary, these protocols fail.

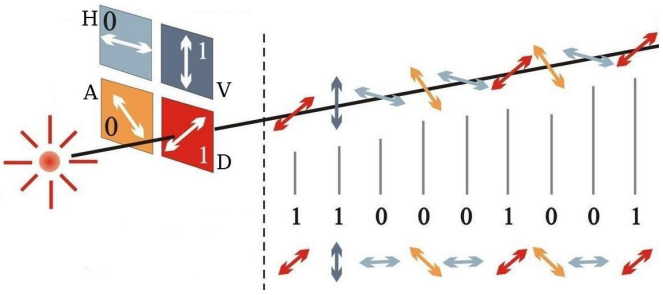


Figure 1.1: BB84 protocol for Quantum Key Distribution: Alice encodes the information in the polarisation of a photon, randomly choosing between two bases. Basis $\{|H\rangle, |V\rangle\}$ is the main basis used to exchange the information on the secret key. Basis $\{|D\rangle, |A\rangle\}$ is used to detect the presence of the eavesdropper.

Quantum computers have been shown to be extremely efficient at solving factorisation problems [**?**] and will easily defeat the RSA protocol. On the other hand, classical random number generators used to produce the secret keys are deterministic and therefore only *pseudo-random*: efficient quantum algorithms for finding patterns in a seemingly random sequence may guess the seed of the generator and at any time predict the bits in the key. Luckily, Quantum Cryptography provides a solution that will allow the exchange of secret keys along a public, untrusted channel with provable unconditional security guaranteed by the laws of Physics and independent of the computational power of a possible eavesdropper.

1.1.2 Quantum Key Distribution

In its most simple implementation, Quantum Key Distribution (QKD) is a quantum version of private key cryptography.

In Quantum Cryptography, quantum information is exchanged in the form of qubits encoded by the sender (usually referred to as Alice) in the quantum state of single photons. The receiver (Bob) decodes the information by performing a quantum measurement on the state.

Several Quantum Key Distribution protocols have been proposed and tested. The most widely employed is BB84 (after Bennett and Brassard who proposed it in 1984 [4]), which exploits two non-orthogonal bases to encode qubits.

A key point in the protocol is the use of single photons and the non-orthogonality of the two encoding bases which allows the parts to detect the presence of an eavesdropper. Two fundamental theorems of Quantum Information state that:

Information gain implies disturbance. *In any attempt to distinguish between two non orthogonal states, information gain is only possible at the expense of introducing a disturbance to the signal.*

No-cloning theorem. *It is impossible to exactly copy an unknown quantum state.*

These results ensure that, by checking for disturbances in their signals, Alice and Bob can quantitatively establish an upper bound on the information that may be

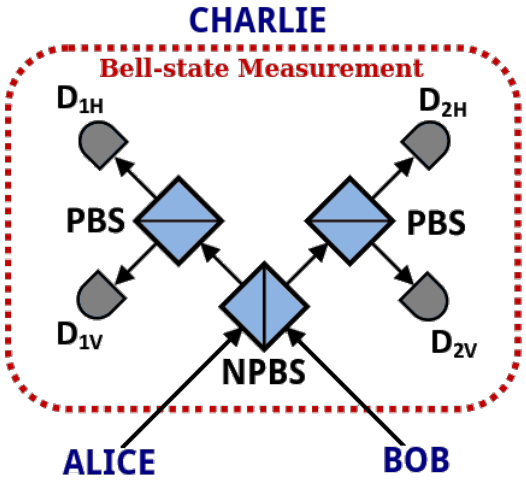


Figure 1.2: MDI-QKD scheme: For polarisation encoding, at the measurement device signals from Alice and Bob interfere at a 50:50 beam-splitter (NPBS) followed by two polarizing beam-splitters (PBS) which project the input photons into either horizontal (H) or vertical (V) polarization states, then detected by four single-photon detectors.

available to the eavesdropper.

1.1.3 Measurement-Device-Independent QKD

Direct Quantum Key Distribution may however suffer from loopholes in the detection of the eavesdropper. These can actually be eliminated, as was first suggested by Ekert in 1991 [5], by exploiting *Entanglement* to test for the presence of an eavesdropper. Subsequent work by [**?**] proposed a Device-Independent QKD scheme where a source of entangled qubits is located between the sender and the receiver, and a secret key is generated by performing a Bell-state measurement on the received entangled state. This would provide the parts with non-local correlations, i.e., correlations that cannot be reproduced by shared randomness (local variables), and the eavesdropper's influence may be quantified by the amount of violation of a Bell-type inequality. DI-QKD requires photon detectors with a near-unitary efficiency and is therefore not realisable with the currently available technology. However, it is possible to perform Measurement-Device-Independent QKD, proposed by [6].

In MDI-QKD, both Alice and Bob prepare a string of random qubits and send them to an untrusted relay (Charlie) located in the middle, who performs a Bell state measurement that projects the incoming signals onto an entangled Bell state. Contrary to DI-QKD, MDI-QKD does not require single photon states, instead it can be performed with weak coherent pulses (WCP) containing an average number of photons $\mu \sim 1$. A successful Bell-state measurement corresponds to the observation of coincident counts in two of the detectors (associated to orthogonal polarisations).

Thus, a key bit is generated if Alice's and Bob's qubits are encoded in the same basis and correspond to orthogonal states. For BB84, this would correspond to the pairs $\{|A\rangle, |D\rangle\}$ and $\{|H\rangle, |V\rangle\}$ and Alice's key is the complementary of Bob's.

From the information on the coincidence counts, which can be publicly shared by

Coincidence	Bell state
$D_{1H} \wedge D_{2V}$	$\|\psi^-\rangle = 1/\sqrt{2}\,(\|HV\rangle - \|VH\rangle)$
$D_{1V} \wedge D_{2H}$	$\|\psi^-\rangle$
$D_{1H} \wedge D_{1V}$	$\|\psi^+\rangle = 1/\sqrt{2}\,(\|HV\rangle + \|VH\rangle)$
$D_{2H} \wedge D_{2V}$	$\|\psi^+\rangle$

Table 1.1: Coincidence table for the Bell-state measurement

Charlie, Alice and Bob can then establish a correlation between their qubits and extract a secret key. Unlike direct QKD, the key bits are not directly encoded in the string measured by Bob, but the information on the key is only created after a successful Bell-state measurement. In order to guess the key, the eavesdropper would need both the information on the coincidence counts, and the information on the two strings that are being sent by Alice and Bob. Since their laboratories are well shielded and they exchange states with a subunitary mean photon number, the eavesdropper cannot gain information by the mere coincidence counts, nor can he gain it by intercepting the flying qubits, as no information is encoded in them unless a successful Bell-state measurement is performed.

1.1.4 Memory-assisted MDI-QKD

Memory-assisted-MDI-QKD is an extension of MDI-QKD, which inherits its resilience against detector attacks, and enhances its rate scaling.

MDI-QKD can only generate key bits if a successful Bell-state measurement is performed, and this presumes that the two single photons arrive at the interfering beam-splitter synchronised. In an out-of-the-lab implementation, the length of the two communication channels may not always be identical, or even stabilised. In MA-MDI-QKD, the photons transmitted by the users are stored each in a QM before the Bell-state measurement. This allows the pulses to be dynamically sincronised and the protocol to work even for communication channels that in principle differ by kilometers (for storage times of the order of $10\mu s$). The performance of such a scheme is moreover enhanced if the storage in the quantum memory can be *heralded*. In such a scheme, when a memorisation event occurs an additional "heralding" photon is emitted by the quantum memory and, by implementing a coincidence setup, it is possible to filter only the actual memorisation events and discard noise.

1.2 Electromagnetically Induced Transparency

Quantum memories (QMs), are quantum light-matter interfaces capable of receiving, storing and retrieving photonic qubits with a higher fidelity than any classical device. Before moving on to explaining the design and operation of

quantum memories, it is useful to focus on understanding the theory behind the storage of photons with room-temperature Rb-vapour cells, the type of quantum memories analysed in this work. At the heart of the operation of such memories is a coherent quantum-optical phenomenon called Electromagnetically-induced transparency (EIT), first observed by Harris in 1991 [7].

1.2.1 Atomic model, dressed states and quantum interference

One of the possible level schemes that produce EIT is the Λ-like hyperfine scheme, as pictured in Figure (1.3), where $|2\rangle$ is a long-lived metastable state and the ground state $|1\rangle$ is separated from state $|2\rangle$ by a dipole-forbidden transition. The control field Ω_C and the probe field Ω_P are respectively coupled to the $|2\rangle \rightarrow |3\rangle$ and $|1\rangle \rightarrow |3\rangle$ transitions. $\Delta_P = \omega_{31} - \omega_P$ and $\Delta_C = \omega_{32} - \omega_C$ represent the one-photon detuning from resonance for the probe and control fields, while δ is the two-photon detuning. γ_{31} and γ_{21} represent the decoherence rates of the two excited states. The essential features of EIT and its application to the storage of

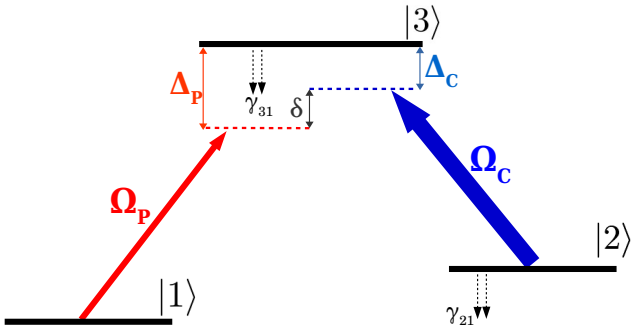


Figure 1.3: Λ-like hyperfine atomic level scheme

photons can be quantitatively described using a semiclassical analysis in which the atom is treated as a quantum system, while the fields are classical. The evolution of the atom-field system under EIT requires this description in terms of state-amplitude or density-matrix equations as the control field induces a strong coupling with the atomic states and the information on the phase and coherence of the states can no longer be ignored. This is in contrast with the rate-equation treatment of state populations which is appropriate when the coupling is weak.

The coupled Hamiltonian of the three-level system can be written in matrix form using the rotating-wave approximation (derived in detail in [?]) as:

$$H_{EIT} = -\frac{\hbar}{2}\begin{bmatrix} 0 & 0 & \Omega_P \\ 0 & -2\delta & \Omega_C \\ \Omega_P & \Omega_C & -2\Delta_P \end{bmatrix} \tag{1.1}$$

where $\Omega_{P,C} = \frac{\mu E_{P,C}}{\hbar}$ is the Rabi frequency of the probe and control fields.
The eigenstates of the *dressed* atom (i.e. after coupling with the control field)

can be written in terms of the mixing angles ϑ and ϕ and the *bare* atomic states:

$$\tan\vartheta = \frac{\Omega_P}{\Omega_C} \qquad \tan 2\phi = \frac{\sqrt{\Omega_P^2+\Omega_C^2}}{\Delta} \tag{1.2}$$

$$|a^+\rangle = \sin\vartheta\sin\phi\,|1\rangle + \cos\phi\,|3\rangle + \cos\vartheta\sin\phi\,|2\rangle \tag{1.3}$$
$$|a^-\rangle = \sin\vartheta\cos\phi\,|1\rangle - \sin\phi\,|3\rangle + \cos\vartheta\cos\phi\,|2\rangle \tag{1.4}$$
$$|a^0\rangle = \cos\vartheta\,|1\rangle - \sin\vartheta\,|2\rangle \tag{1.5}$$

The new gound-state $|a^0\rangle$ contains no component of state $|3\rangle$ and this results in the coherent population trapping in state $|3\rangle$. In other words, the control field pumps electrons from state $|2\rangle$ to state $|3\rangle$. The probe field can be absorbed via two main different excitation pathways ($|1\rangle \to |3\rangle$ or $|1\rangle \to |3\rangle \to |2\rangle \to |3\rangle$) but thanks to the presence of the control field, the combined amplitudes of the two processes interfere destructively and the probe field is not absorbed.
In the case of a weak probe field, $\Omega_P \ll \Omega_C$ and $\delta = 0$ the dressed states become:

$$\tan\vartheta = \frac{\Omega_P}{\Omega_C} \qquad \tan 2\phi = \frac{\sqrt{\Omega_P^2+\Omega_C^2}}{\Delta} \tag{1.6}$$

$$|a^+\rangle = \tfrac{1}{\sqrt{2}}\left(|2\rangle + |3\rangle\right) \tag{1.7}$$
$$|a^-\rangle = \tfrac{1}{\sqrt{2}}\left(|2\rangle - |3\rangle\right) \tag{1.8}$$
$$|a^0\rangle = |1\rangle \tag{1.9}$$

1.2.2 The ensemble density operator

The *dressed* state picture presented so far can be generalised to describe a statistical ensemble of atoms and their interaction with optical fields. The Von Neumann equation (1.10) gives the evolution in terms of the ensemble's density matrix ρ.

$$\dot{\rho} = -\frac{i}{\hbar}\left[H,\rho\right] - \frac{1}{2}\left\{\Gamma,\rho\right\} \tag{1.10}$$

where the second term represents the decoherence caused by the spontaneous decay of the excited states $|3\rangle$,$|2\rangle$ and H is the same of equation (1.1).
Assuming that $\gamma_{21} \ll \gamma_{31}$, by solving the equation we find:

$$\rho_{11} \approx 1$$
$$\rho_{22} = \rho_{33} \approx 0$$
$$\rho_{12} = \rho_{21}^* = \frac{\Omega_C\Omega_P}{4(i\gamma_{21}+\Delta_C-\Delta_P)(-i\gamma_{31}+\Delta_P)+\Omega_C^2}$$
$$\rho_{13} = \rho_{31}^* = \frac{2(\gamma_{21}-i(\Delta_C-\Delta_P))\Omega_P}{4(\gamma_{31}+i\Delta_P)(-i\gamma_{21}-\Delta_C+\Delta_P)-i\Omega_C^2}$$

The linear response of the medium near the resonance is then given by $\chi^{(1)}$:

$$\chi^{(1)} = \frac{2N|\mathcal{P}_{31}|}{\mathcal{E}_P\varepsilon_0}\rho_{13} \tag{1.11}$$

where $\mathcal{P}$ represents the dipole momentum.

1.2.3 A fully quantum treatment: dark-state polaritons and adiabatic preparation

In order to better understand the effect of a time-varying control field on the propagation of the probe field, it is necessary to adopt a full quantum treatment of both fields and atoms, as done by Fleischhauer and Lukin in [1].
A crucial assumption is that the control field is varied slowly, so that the interaction with the atomic ensemble is adiabatically and coherently controlled. Furthermore, if the probe field is much weaker that the control field, $\mathcal{E}_P$ can be treated as a perturbative term and we may write the propagation equation for $\hat{\mathcal{E}}_P(z,t)$ as:

$$\left(\frac{\partial}{\partial t} + c\frac{\partial}{\partial z}\right)\hat{\mathcal{E}}_P(z,t) = -\frac{g^2 N}{\Omega_C(t)}\frac{\partial}{\partial t}\left(\frac{\hat{\mathcal{E}}_P(z,t)}{\Omega_C(t)}\right) \tag{1.12}$$

where g is the atom-field coupling constant: $g = \mathcal{P}\sqrt{\frac{\nu}{2\hbar\varepsilon_0 V}}$.
If $\Omega_C = const$, the right-hand-side term of the equation leads to a reduction in the group velocity of the pulse to:

$$v_g = \frac{c}{1 + \frac{g^2 N}{\Omega_C^2}} \tag{1.13}$$

In general, if Ω_C varies in time, the quantum field equation acquires a term that corresponds to a reversible change in the field amplitude. Indeed, a simple solution of the propagation equation is obtained by introducing a new quantum field $\hat{\psi}(z,t)$, corresponding to a quasi-particle collective spin-wave excitation of the medium, *dark-state polariton*, via the canonical transformation:

$$\hat{\psi}(z,t) = \cos\vartheta(t)\hat{\mathcal{E}}_P(z,t) - \sin\vartheta(t)\sqrt{N}\hat{\rho}_{12}(z,t) \tag{1.14}$$

where:

$$\cos\vartheta(t) = \frac{\Omega_C(t)}{\sqrt{\Omega_C^2 + g^2 N}} \tag{1.15}$$

$\hat{\psi}$ obeys the equation of motion:

$$\left[\frac{\partial}{\partial t} + c\cos^2\vartheta(t)\frac{\partial}{\partial z}\right]\hat{\psi}(z,t) = 0 \tag{1.16}$$

which corresponds to a shape-preserving propagation with group velocity $v_g = c\cos^2\vartheta(t)$.
Thus, the photonic quantum state can be coherently and reversibly mapped into a collective atomic excitation by adiabatically rotating ϑ from 0 to $\pi/2$ by changing the strength of the control field, thus enabling the timed *writing* and *reading* of the pulse out of the quantum memory.

1.2.4 EIT at room temperature

Typically, the observation of coherent phenomena in atomic media is hindered by dephasing caused by collisions and inhomogenoeus broadening due to the Doppler

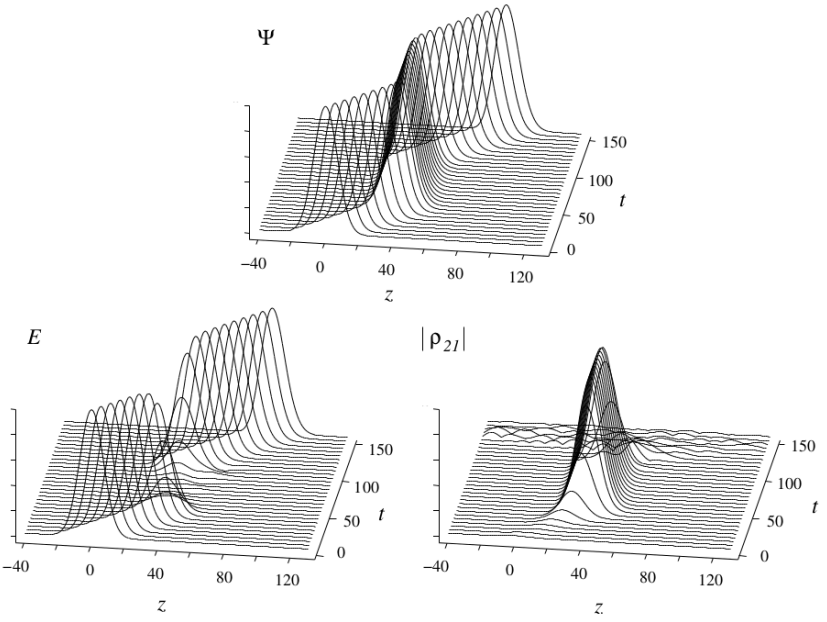


Figure 1.4: Evolution of the dark-state polariton $\hat{\psi}$ (top), probe field $\hat{\mathcal{E}}_P$ (bottom-left), and atomic excitation $\hat{\rho}_{12}$ (bottom-right). From [1].

effect. EIT, however, can be successfully exploited to store single photons even at room temperature. The key to room-temperature operation is that, during storage, the information encoded in a single photon is not transferred to a single atom, but to a collective excitation of the medium. A single photon interacts with the whole atomic ensemble and the dark-state polariton created in the process has a gaussian amplitude inside the volume.
Decoherence poses a limit on the maximum length of the cell, but as long as the decoherence rates satisfy $\gamma_{21} \ll \gamma_{31}$, EIT can be sustained. Furthermore, at room temperature the Doppler effect gives a substantial contribution to the broadening and shifting of the resonance. By exploiting a hyperfine level system and making sure that the probe and control field propagate collinearly, we can ensure that the two lines are Doppler-shifted in the same way and that the Doppler effect cancels out.

1.2.5 Macroscopic properties

From a macroscopic point of view, EIT results in a strong modification of the linear susceptibility of the atomic medium. The linear susceptibility $\chi^{(1)}$ is defined as:

$$\vec{P} = \epsilon_0 \chi^{(1)} \vec{E} \tag{1.17}$$

The imaginary part of $\chi^{(1)}$, $\Im\left[\chi^{(1)}\right]$ determines the dissipation and absorption of the field and, for a dipole-allowed transition, it follows a Lorentzian function with a width set by the damping. The real part $\Re\left[\chi^{(1)}\right]$ instead determines the refractive index and group velocity. Without EIT, $\Re\left[\chi^{(1)}\right]$ follows the standard dispersion profile, with anomalous dispersion at the absorption peak. $\Im\left[\chi^{(1)}\right]$

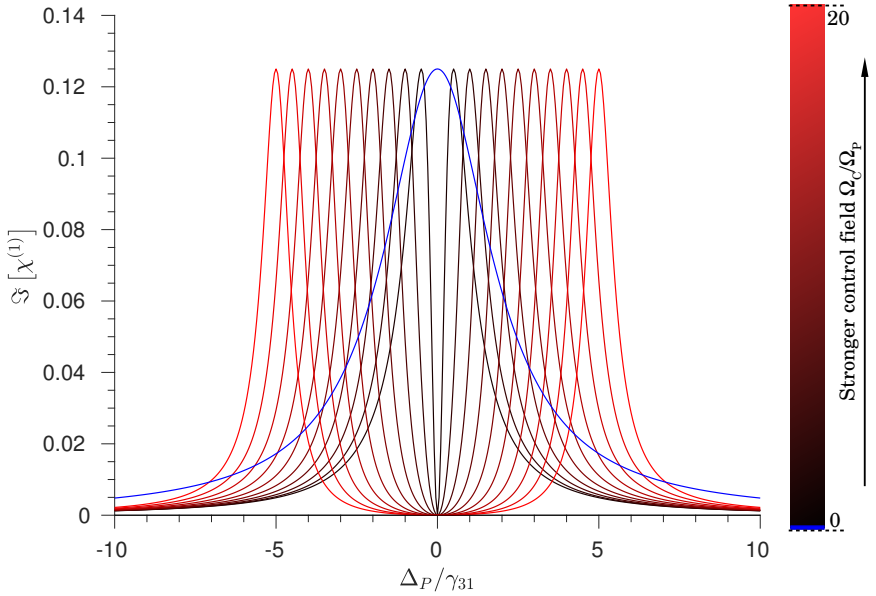


Figure 1.5: Imaginary term of the linear susceptibility $\chi^{(1)}$ under conditions of EIT as a function of the probe field detuning Δ_P, normalised over the dephasing rate γ_{31}, under the assumption of weak decoherence: $\gamma_{21} = 10^{-4}\gamma_{31}$. The transparency window widens increasing the relative strength of the control field. The blue line corresponds to $\Omega_C = 0$.

undergoes destructive interference in the region of resonance of the probe field ($\Delta_P = 0$), which results in the medium being perfectly transparent to probe light. This fact is not important in itself, but rather in conjuction with the fact that the third-order susceptibility $\chi^{(3)}$ displays instead a constructive interference peak. Under EIT, $\Re\left[\chi^{(1)}\right]$ displays steep normal dispersion instead of the standard less steep anomalous dispersion. These changes in the response of the medium give rise to a sharp reduction of the medium group velocity v_{gr}, down to 10m/s for cryogenic EIT with high optical densities.

$$v_{gr} = \left.\frac{d\omega_P}{dk_P}\right|_{(\Delta_P=0)} = \left.\frac{c}{n + \omega_P \frac{dn}{d\omega_P}}\right|_{(\Delta_P=0)} \tag{1.18}$$

At the resonance, the refraction index is $n = 1$ and therefore the phase velocity in the medium is the same as in vacuuum. The second-order susceptibility $\chi^{(2)}$ vanishes at resonance and this results in no group velocity dispersion. The ultra-slow group velocity also induces a strong spatial compression of the pulse in the longitudinal direction, with a ratio of v_{gr}/c.
If we include the effect of decoherence, the window in $\Im\left[\chi^{(1)}\right]$ loses transparency and the transition becomes smoother.

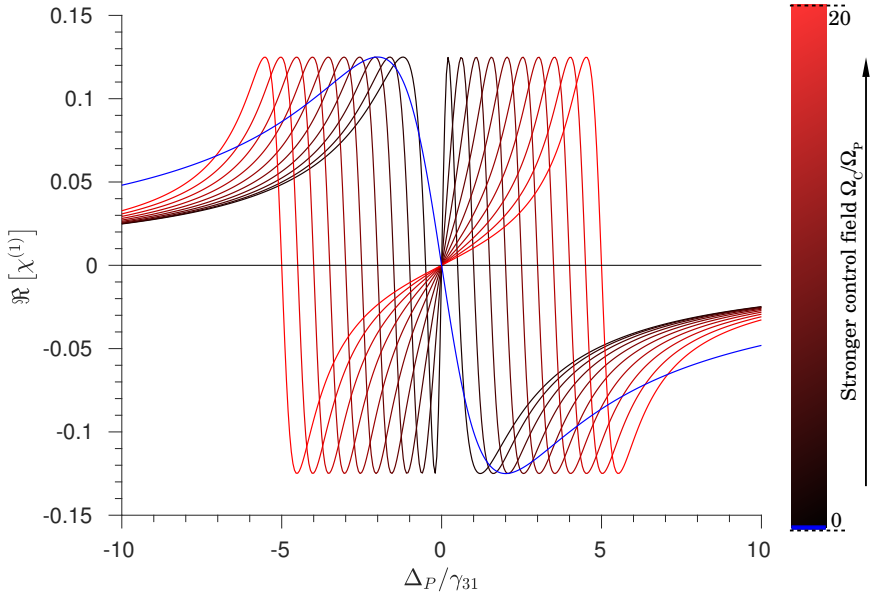


Figure 1.6: Real term of the linear susceptibility $\chi^{(1)}$ under conditions of EIT as a function of the probe field detuning Δ_P, normalised over the dephasing rate γ_{31}, under the assumption of weak decoherence: $\gamma_{21} = 10^{-4}\gamma_{31}$. The slope of the curve changes sign with the onset of EIT, from standard anomalous dispersion to steep normal dispersion. Increasing the relative strength of the control field, the curve becomes less steep. The blue line corresponds to $\Omega_C = 0$.

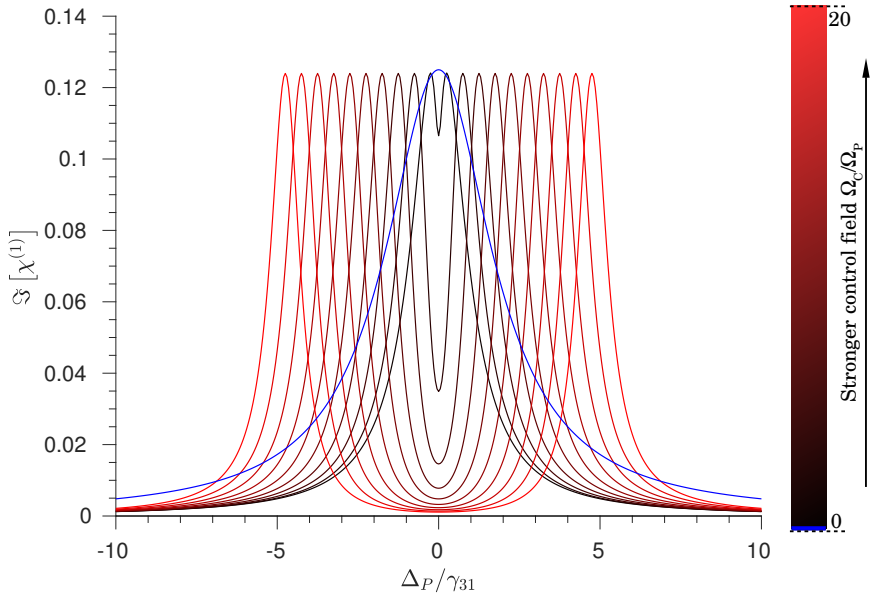


Figure 1.7: $\Im\left[\chi^{(1)}\right]$ with stronger decoherence: $\gamma_{21} = 10^{-1}\gamma_{31}$

1.3 Quantum Memories

This work is specifically focused on room-temperature Rb-vapor quantum memories, which exploit electromagnetically-induced transparency to store photons.

1.3.1 Overview of quantum memory designs

Over the past 10 years, several diverse approaches exploiting different physical effects have been proposed and studied [8],[9], such as: atomic frequency comb memories (AFC) based on solid-state atomic ensembles in rare-earth doped crystals, Nitrogen vacancy (NV) centers in diamond, semiconductor quantum dots, single trapped atoms in cavities, room-temperature and cold atomic gases exploiting Raman transitions or electromagnetically induced transparency, and optical phonons in bulk diamond. Some of these designs have already demonstrated quantum features such as the ability to store qubits and entanglement. Important parameters in assessing the design's performance are the QM's fidelity, efficiency, storage time, bandwidth and the conditions on its operation environment. All approaches appear to be suitable in principle for high-fidelity and high-efficiency operation, but complexity and all-environment operation are ultimately important and pose technological challenges for a future large-scale implementation.

Fidelity. The most important parameter for the correct operation of the QM is the fidelity, i.e., the ability of the QM to preserve the quantum state's wavefunction after storage.
It's interesting to note that the information on the quantum state is coherently transferred to the QM during the storage process, and the state is not directly measured. The opposite happens for a "classical memory" where the state is intercepted, measured and resent. Such a strategy comes at odds with the quantum no-cloning theorem, which strictly limits the maximum fidelity to $F = 71 - 83.6\%$. A QM, on the other hand, can in a sense defeat the quantum no-cloning theorem and achieve $F = 100\%$.

Efficiency. Efficiency is defined as the probability to re-emit a photon that has been stored. In cold atomic ensembles the efficiency can in principle be close to one thanks to collective interference effects, while for warm-atomic vapour systems the efficiency can be as low 1%.

Storage time. This is a critical parameter for applications in quantum communication, as it determines the maximum channel length difference that can be compensated by the QM in a MA-MDI-QKD scheme. The longest storage times achieved in cryogenic systems are in the range of ms to s.

Bandwidth and wavelength. Wavelength is particularly important when considering the available photon sources and the requirements of the communication channel in which the memory is to be introduced. For free-space channels, no limitations apply, whereas for fiber-optic links the wavelength needs to match the fiber's transparency window. Most implementations aim for bandwidths in the range of 100MHz to 1GHz.

Capacity to store multiple modes. This is capability may allow a multiplication of the repetition rate, which may be useful in QKD where the bit-rate of the communication has to be kept high (1GHz) in order to overcome the losses in the channel and achieve a positive key-rate.

Complexity This is the decisive requirement for large-scale operation. Most solid-state implementations require cryostats and micro- or nanofabrication, while atomic approaches may require laser cooling and trapping. On the other hand, room temperature QMs with vapor cells benefit from easy operation without the need for laser cooling and trapping, promoting the scalability.

1.3.2 Room-temperature Rb-vapour Quantum Memory for polarisation qubits

The application of EIT to the storage of photons was first put forward by Fleischhauer and Lukin in 2000 [1]. The first Rb-vapor quantum memory for storage of an arbitrary polarisation state working at room temperature was realised by Figueroa and collaborators in 2014 [10] and it is on this design that the present work is based.

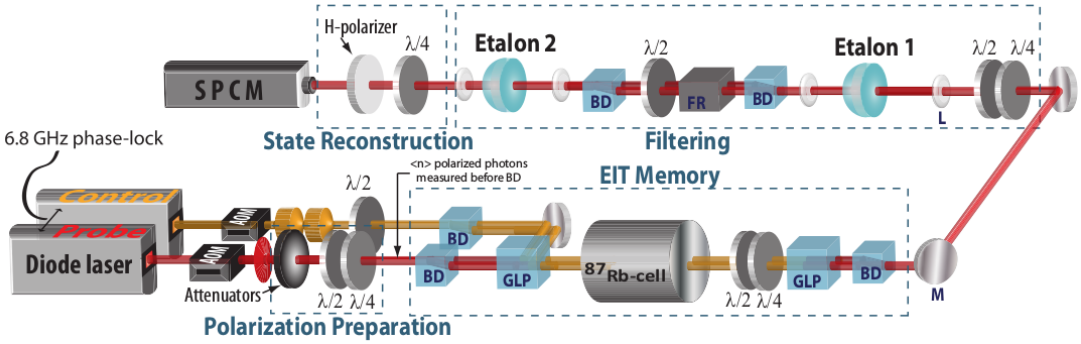


Figure 1.8: Dual-rail QM setup for storage of arbitrary polarisation qubits in a warm Rb vapour cell under EIT

Frequency locking

A crucial element in the setup is the frequency locking of the probe and control fields, without which EIT cannot happen. In the case of Rubidium, the probe and control field are locked to two hyperfine-split transitions. The probe field frequency is stabilized to the $5S_{1/2}F = 1 \rightarrow 5P_{1/2}F = 1$ transition at a wavelength $\lambda = 795$ nm which corresponds to a frequency of $\nu = 377\ THz$ while the control field interacts with the $5S_{1/2}F = 2 \rightarrow 5P_{1/2}F = 1$ transition. The frequency difference between states $|2\rangle$ and $|1\rangle$ is $\Delta\nu = 6.835$ GHz. Both lines are inhomogeneously broadened by the Doppler effect and this ensures that EIT can happen even at large one-photon detunings $\Delta_{P,C}$ as long as the two-photon detuning is locked at $\delta = 0$. This is achieved by phase-locking the control field to a frequency difference equal to the separation of the two lines, $\Delta\nu$. The bandwith of the EIT process is 1MHz and, by repeatedl mixing the signal, the locking is achieved with a precision of the order of the kHz.

Rubidium cell

At the heart of the setup is the Rubidium cell. The cell contains a vapour of

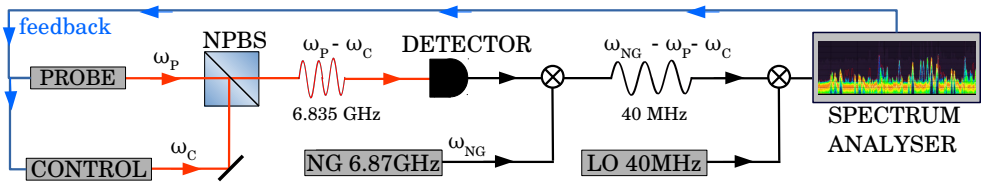


Figure 1.9: Schematic of the phase-locking setup used to lock the probe and control fields to the proper transitions for EIT. The probe and control laser interfere at a beam splitter, thus generating a beat note at a frequency equal to their frequency difference, 6.835 GHz. The signal is read by a photodiode and subsequently mixed with an electrical signal from a local oscillator at 6.8 GHz to produce a beat note at 40 MHz, before being fed to a feedback network which filters and locks the phase.

^{87}Rb and Kripton gas. The role of Kr is to act as a buffer and reduce the collisions between Rb atoms which would result in dephasing and decoherence of EIT. The cell is heated at a temperature of $60°C$. It is crucial that the cell be heated uniformly, otherwise Rb might condensate on the surface and degrade the visibility and performance of the cell. The cell also needs to be shielded from electro-magnetic noise present in the environment.

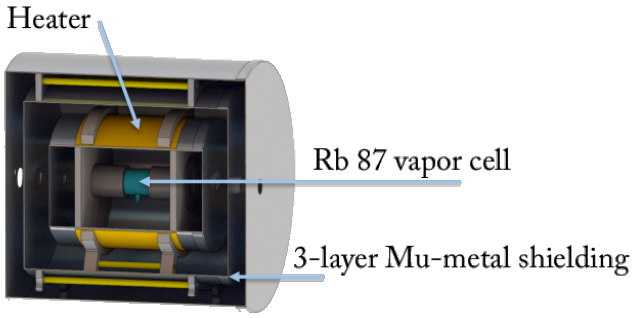


Figure 1.10: Section of the Rubidium cell showing the heating and shielding layers

Dual-rail operation

Storage via EIT does not strictly preserve the polarisation, however, the two orthogonal components can be mapped into two spatially distanced beams in a dual-rail configuration where two independent coherently prepared volumes exist in the same Rb-cell.

Filtering system

EIT requires the control field to be much stronger tha nthe probe signal, therefore it is necessary to introduce a filtering setup after the Rb-cell, which needs to provide at least 102dB of the control field suppression. The setup is composed of a polarising beam splitter, which reflects the control field (polarised $|V\rangle$, orthogonal to the $|H\rangle$ probe field which is transmitted) and two etalon resonators with a bandwidth of 40 and 24 MHz, respectively. The wavelength separation between the probe and control field is so narrow ($\Delta\lambda \sim$ 1pm) that the etalons are not simply aligned, as this would not be sufficient, but their thickness is temperature-controlled. The effective control/probe suppression ratio is 130dB. A Faraday

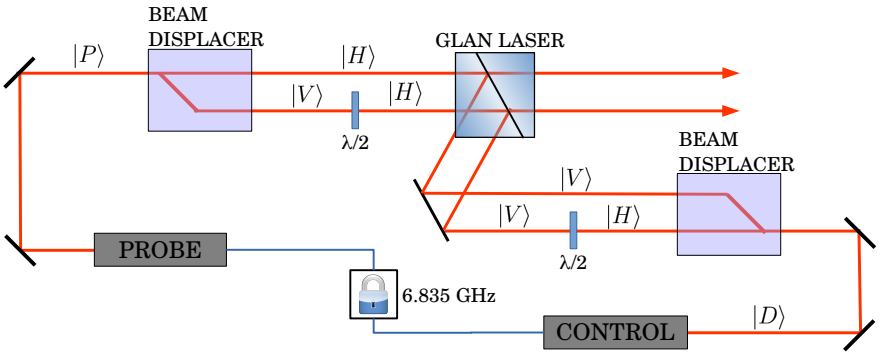


Figure 1.11: The arbitrary polarisation state of the probe field is mapped into two spatial modes by a beam displacer and overlapped with the control field (whose polarisation is fixed on $|D\rangle$) after a Glan laser polariser.

isolator is placed between the two etalons to prevent back-reflection from the second etalon from damaging the first.

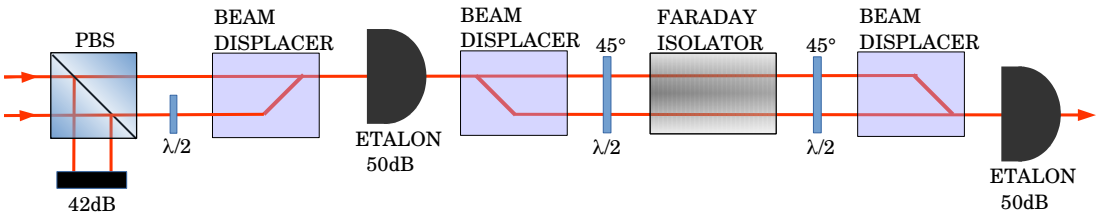


Figure 1.12: Schematic of the filtering setup: first a polarising beam-splitter reflects the control field, providing 42dB extinction, then two etalon resonators screened by a Faraday isolator provide 50dB each.

2 Outline and goals of this work

2.1 Context

The present work fits in the broader framework of an ongoing collaboration between the QuantumFuture research group at the University of Padova, and the Quantum Information and Technology group at Stony Brook University (NY,USA). The main expertise of the group in Padova is Quantum Communication, while Stony Brook focuses its research on the development of room-temperature Quantum Memories.

A joint experiment conducted at Stony Brook in 2016 demonstrated the operation of a functional elementary quantum network by combining free-space propagation of random single-photon level BB84 polarisation qubits and their storage and retrieval in a room-temperature quantum memory.
Weak coherent pulses were generated with acousto-optic modulators (AOMs) at the single photon level encoding polarisation states in a randomised sequence. The random qubits were sent over a 20m-long free-space link and coupled into a dual-rail room-temperature quantum memory and after storage and retrieval were analysed in a four-detector setup. With a bare quantum memory operation

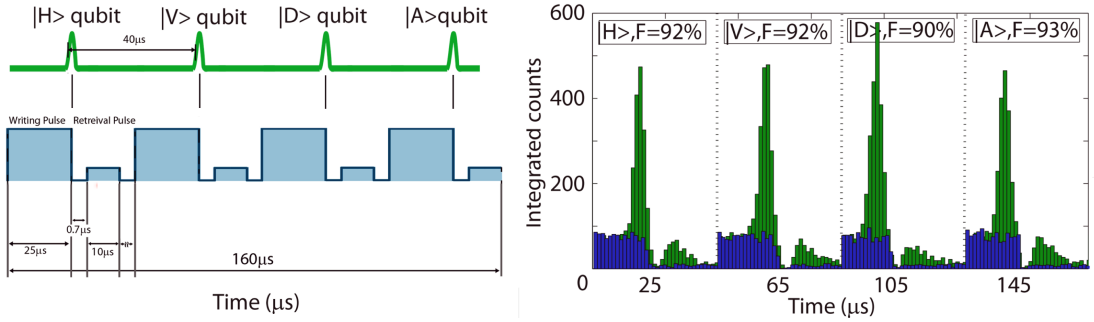


Figure 2.1

a QBER = 11.9% was achieved for $\mu = 1.6$. This value lies just outside of the region for positive key rate generation, indicating not fully-secure communication. By applying noise reduction techniques the QBER was lowered to 3% for $\mu = 1$,

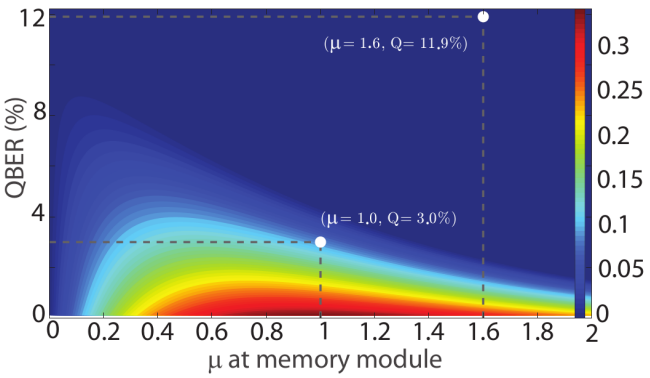


Figure 2.2: QBER vs mean photon number, colour-coded by key generation rate. The intersection between light blue and dark blue (negative key rate area) corresponds to the boundary for the positive key rate. The white dots indicate the bare and noise-free regimes. From [2]

which is well above the secure communication threshold.

2.2 Objectives

Building on the results of the 2016 experiment, the two groups are continuing the collaboration with the ultimate goal of realising MA-MDI-QKD where the Bell-state measurement is assisted by two quantum memories, one for each channel.

An intermediate goal, which is covered in this thesis, is to observe classical interference and Hong-Ou-Mandel (HOM) two-photon interference between weak coherent pulses after storage in a room-temperature quantum memory.

2.3 Challenges and methods

Twin qubit sources The previous experiment used four beams pulsed by four AOMs to produce the four polarisation states and the frequency of switching was limited to 20kHz. In order to increase the switching frequency and simplify the design, it is better to use an electro-optic modulator (EOM), which can directly modulate the polarisation of a single beam, together with an AOM, which is used for pulsing. EOMs are very sensitive to alignment, which needs to be optimised in order to produce the correct polarisation modulation.

Quantum memory The setup and parameters of the quantum memories should ensure optimal fidelity in for the storage of polarisation qubits.

HOM interference setup Two-photon interference arises from the indistinguishability of two photons in different paths and therefore requires precise alignment, mode-matching, stabilised polarisation and a time-coincidence setup.

Driver and control electronics for QKD With QKD applications in mind, the EOM needs a driver able to switch between four high voltage levels (in the range $0 - 500$V) with suitable frequency and duty cycle and low ripple.

In addition, the system needs a digital interface, implemented on an FPGA, which produces the triggers for the four voltage levels of the EOM driver, for the AOM and for the detectors.

3

Setup of the twin qubit sources

The setup of the two qubit sources (Alice and Bob) is identical. The light for both Alice and Bob is derived from the same laser source at 795nm, which is locked to a control laser with a frequency difference of 8.35GHz. Two acousto-optic modulators (AOMs) generate two gaussian pulses 400ns-long with a repetition rate of 20kHz. AOMs are driven by a frequency modulation and an amplitude modulation, which can be set on a DC level for CW operation. Because of the frequency modulation at ν=80MHz, the AOMs produce three output beams with frequency shifts $\{-\nu, 0, +\nu\}$.

An iris selects the $+\nu$ component for both Alice and Bob, and these are then coupled into two polarisation-maintaining (PM) fibers that reach the electro-optic polarisation setup. The mode entering the PM fiber is aligned at coupling with the fast axis of the fiber, so that the polarisation at the output is stable with more than 50dB of extinction ratio. At the output of the fiber, a half wave-plate rotates the polarisation to horizontal while a polariser and quarter waveplate eliminate any residual ellipticity.

The electro-optic polarisation modulator (EOM) is a Pockels cell type modulator and consists of two lithium niobate (LiNbO3) crystals. Voltage applied across the crystal structure induces change in the indices of refraction (both ordinary and extraordinary), leading to an electric field dependent birefringence. An optical wave with polarisation components on both the ordinary and extraordinary axes of the crystal will experience a change in polarisation state arising from the relative phase delay between the orthogonal components. Thus, the electro-optic crystal acts as a variable waveplate with retardance linearly dependent on the applied voltage.

Lithium niobate exhibits a static temperature-dependent birefringence which may cause variations in the output polarisation. To minimize this effect, the two lithium niobate crystals are rotated 90° one with respect to the other so that the static birefrincence induced by the first is cancelled by the second crystal. This way, the temperature sensitivity of the crystal is typically $< 1mrad/^{\circ}C$. In order for the EOM to produce the correct polarisation modulation, the beam needs to

Polarisation	$\|H\rangle$	$\|L\rangle$	$\|V\rangle$	$\|R\rangle$
Voltage	0V	$\frac{1}{2}V_\pi = 131.6V$	$V_\pi = 263.2V$	$\frac{3}{2}V_\pi = 394.7V$

Table 3.1: EOM voltages and corresponding polarisation shifts

be aligned orthogonally to the ordinary and extra-ordinary axes of the crystal. The voltage required to produce a polarisation shift of π is called the half-wave voltage and is given by:

$$V_\pi = \frac{\lambda}{n_E^2 r_{33} - n_O r_{13}} \frac{d}{L} \tag{3.1}$$

where r_{33} and r_{13} are the Pockels coefficients and d and L are the thickness and length of the crystal. The indices of refraction are themselves functions of the wavelength and temperature, however, for room-temperature operation the formula can be simplified as:

$$V_\pi = 0.361\lambda_{[nm]} - 23.844V \tag{3.2}$$

Assuming an input horizontal polarisation $|H\rangle$ and a wavelength of 795nm, the voltages required to produce the four states employed in the BB84 protocol are: The $|L\rangle$ and $|R\rangle$ polarisation states correspond to left-handed and right-handed circular polarisations and can be transformed to $|A\rangle$ and $|D\rangle$ states by a quarter waveplate placed at the output of the EOM and aligned parallel to either $|H\rangle$ or $|V\rangle$.

Although this kind of EOM can handle switching frequencies up to 100MHz, the main drawback associated to it is the fact that it requires high driving voltages and therefore the design of a fast driver for switching applications is not straightforward.

The output of the system is coupled to two 20m-long single-mode optical fibers which reach the quantum memory and interference setup. Single-mode fibers do not preserve the polarisation, and the output state varies depending on the stress and bending applied to the fiber. It is therefore essential to stabilise the fiber so that no accidental change in the polarisation occurs. Without external disturbance, the extinction ratio measured at the output of the fiber is above 40dB, meaning that the polarisation does not change considerably. Most importantly, any two orthogonal input modes remain orthogonal after propagation through a single-mode fiber, which would not have been the case for PM fibers, which only maintain the modes that are aligned to the fast and slow axes.

4 Hong-Ou-Mandel interference with polarisation qubits

4.1 Hong-Ou-Mandel interference

Hong-Ou-Mandel (HOM) interference is a quantum interference phenomenon first observed in 1987 [11] which occurs when two indistinguishable photons are fed to two input ports of a 50:50 beam-splitter. HOM interference is fundamental for MDI-QKD applications.

With classical light, a beam-splitter acts as a power-splitter, by simply dividing the power at the two output ports by the ratio of transmissivity/reflectivity associated to the beam-splitter. In the case of a single photon entering the beam-splitter, because of its indivisibility, the process becomes probabilistic and the photon can either be reflected with probability R, or transmitted with probability $(1 - R)$, where R is the reflectivity of the beam-splitter.

For an input quantum state with a single photon at each port of a R:(1-R) beam-splitter,

$$\psi^{IN} = |1\rangle \otimes |1'\rangle \tag{4.1}$$

the output state is a quantum superposition of four possible cases, each weighted by their probability. In the case of reflection, the output state acquires an i factor.

$$\begin{aligned} \psi^{OUT} = R(1-R)i\,|0\rangle \otimes |1+1'\rangle \quad &+ \quad R(1-R)i\,|0\rangle\,|1+1'\rangle \otimes |0\rangle \\ + (1-R)(1-R)\,|1\rangle \otimes |1'\rangle \quad &- \quad R^2\,|1'\rangle \otimes |1\rangle \end{aligned}$$

For a perfect 50:50 beam-splitter, if indeed the two photons $|1\rangle$ and $|1'\rangle$ are indistinguishable, the last two terms in ψ^{OUT} - corresponding to both photons being either reflected or transmitted - cancel out in destructive quantum interference and the two photons always exit the beam-splitter at the same port. This interference can be measured by observing the coincidence between photons detected at the two outputs. With indistinguishable single-photon Fock states the coincidence counts fall to zero and the visibility of the *HOM dip* is 100%.

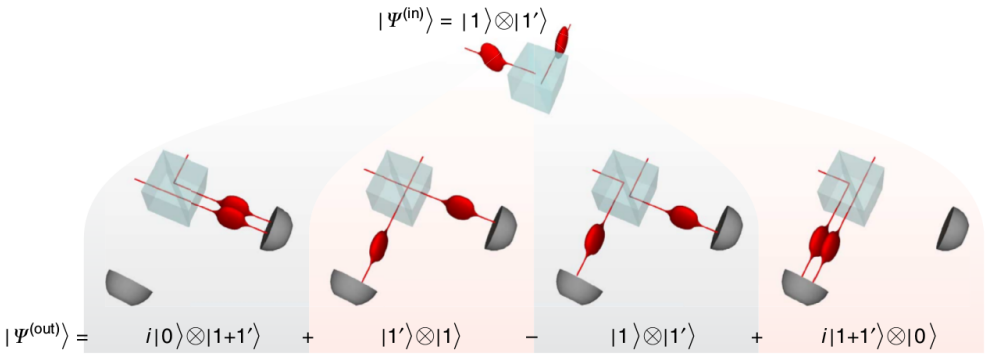


Figure 4.1: HOM interference with single photons

When weak coherent pulses (WCP) obeying Poissonian statistics are fed to the beam-splitter ports the maximum achievable visibility is instead 50% [12], while for an arbitrary reflectivity the maximum visibility is R.

4.2 Setup

In principle, the setup needed to observe HOM interference is simple: a non-polarising beam-splitter (NPBS) and two single-photon counters.

This apparent simplicity hides several pitfalls which stem from the fact that the

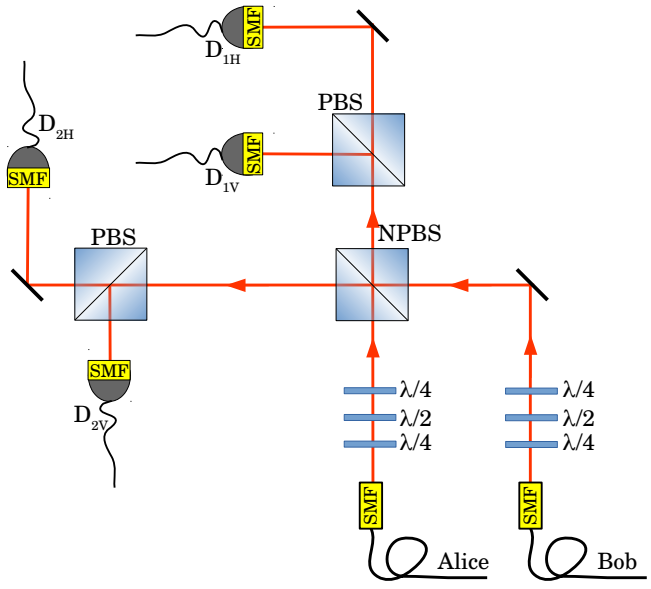


Figure 4.2: Setup for HOM interference

two interfering photons need to be indistinguishable:

Polarisation stability. For the interference to be observable, the two beams need to have the same polarisation. Three compensation plates $\{\lambda/4 - \lambda/2 - \lambda/4\}$ were rotated to (for each beam) minimise the power detected by D_{1V} and D_{2V}, which corresponds to fixing the polarisation on $|H\rangle$ for

both Alice and Bob.
The visibility of $|H\rangle$, defined as the ratio of power measured in the $|H\rangle$ port of the beam-splitter over the total power was optimised at $90 - 98\%$.

Alignment. This is important both for the visibility of the interference and the detection. Improving the alignment results in better visibility of the interference and, given that the single-photon counters are fiber-coupled, equal efficiencies of detection for both beams.

Mode-matching. Once the alignment is ensured, by matching the modes of the two beams, the maximum overlap is achieved at the beam-splitter.

Detection. The coupling efficiency was optimised to increase the SNR.

4.3 Classical interference

The first step towards measuring HOM quantum interference is to measure classical interference between the sources.

As explained in Chapter 3, the AOMs used to generate the light pulses output three beams with $\{-\nu, 0, +\nu\}$ frequency shifts, where ν is the frequency modulation applied to the AOM. By driving Alice's and Bob's AOMs with different frequencies ν and ν', a beat-note sinusoidal modulation at a frequency $\nu - \nu'$ is created after the beam-splitter and this corresponds to classical interference in the time domain.

Clearly, quantum and classical interference are entirely different phenomena, with the first requiring the indistinguishability of photons and the second requiring a frequency difference, yet, quantum interference cannot be observed if the setup is not precisely coupled, matched and aligned so that classical interference can be measured in the first place.

4.3.1 Continuous wave classical interference

The frequencies of the two AOMs were set at 80MHz and 79MHz, so as to create a beat-note modulation at 1MHz. Both outputs of the NPBS are then coupled into a single-mode fiber and the signal was detected using a photodiode.

In addition, a removable mirror can be placed on one of the paths to direct the free-space beam to the photodetector. The free-space measurement is particularly relevant to verify the polarisation stability of the setup: the fiber-coupled outputs are indeed placed after two PBSs needed for the polarisation alignment (and for a future upgrade of the setup to perform a Bell-state measurement) and therefore any polarisation fluctuations would be indistinguishable from input power fluctuations.
Figure (4.3) shows the fluctuations of the free-space fringes over 20ms. The visibility of the fringes is 90%. The ripple observed on the maximum is 4% while the

one measured for the minimum is 0.9%. This is a proof that the residual fluctuations are only due to the power fluctuating at the input of the interferometer, and not to changes in the polarisation. If polarisation fluctuations had been present, the visibility would also be affected and modulated by the fluctuations.

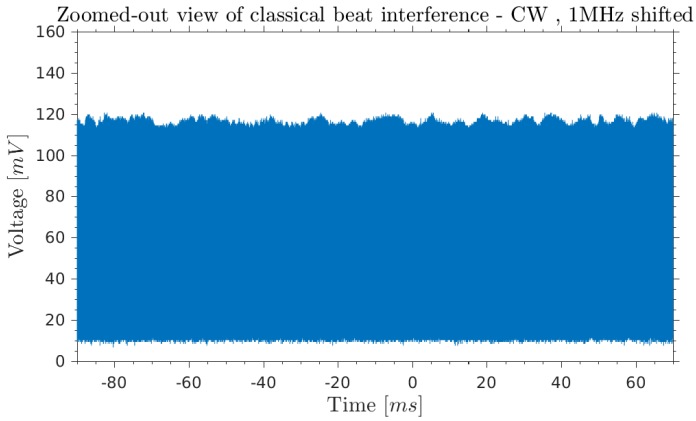


Figure 4.3: Zoomed-out view of the 1MHz beat-note interference fringes for CW operation.

The classical beat-note interference was measured for two 1MHz-shifted beams. The visibility of the 1-MHz modulated fringes is 98%.

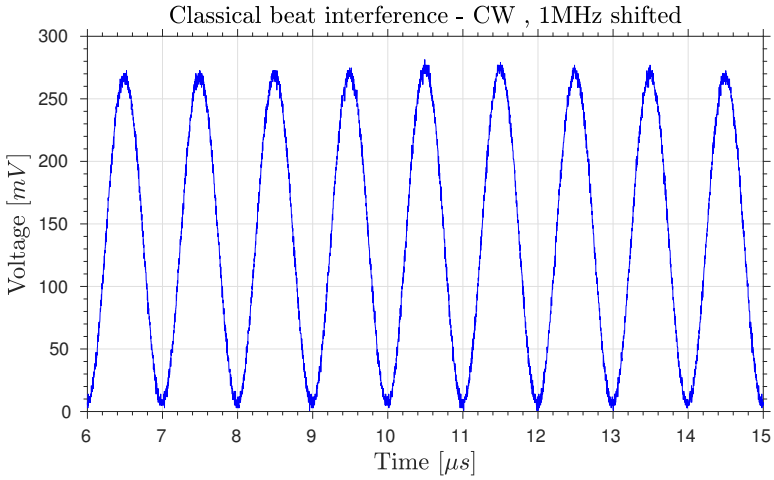


Figure 4.4: Classical interference of two continuous wave beams, 1MHz-shifted in frequency.

4.3.2 Classical interference with pulses

The following step in the measurement was to observe classica beat-note interference with two 400-ns long pulses produced by the sources. In order to observe a modulation in the gaussian pulse, the frequency difference was increased to 5MHz. Figure (4.5) shows the interfering gaussian pulses modulated by the 5MHz fringes.

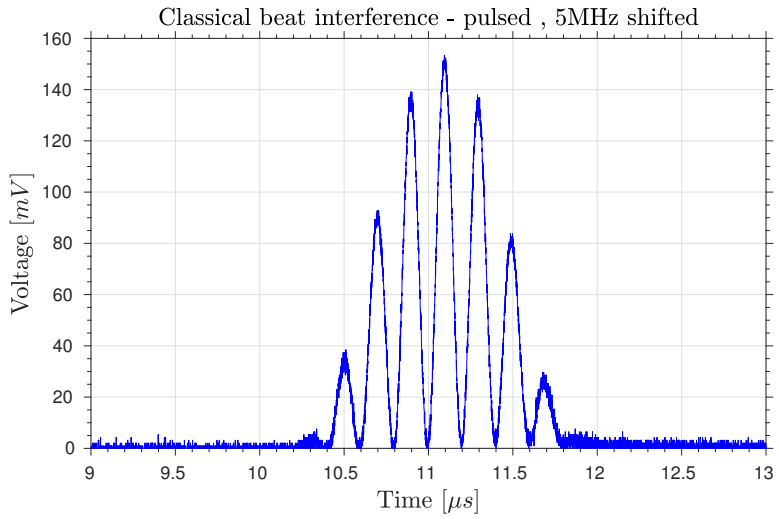


Figure 4.5: Classical interference of two 400ns-long pulses, 5MHz-shifted in frequency.

4.4 Quantum interference

Once the setup was optimised for classical measurements, the optical power emitted by the sources was decreased using an attenuator to produce two weak coherent pulses (WCP) at the input of the interferometer containing less than one photon each. The frequency modulation of the AOMs was set on 80MHz for both sources. The whole setup was screened from background environmental light and the fiber-coupled signal was fed to a single-photon counter.

The signals read from the two photon counters were time-tagged for the coincidence analysis. The ROI (region of interest) for the coincidence analysis was set on an interval of 1.5μs centered on the peak for the unfiltered counts and divided in 100bins, 15ns-long. The data was then filtered to select only the events where a single-photon count was registered both in detector 1 and 2. The result of the filtering is shown in Figure (4.7).

In the case of HOM with single-photon Fock states, the coincidence counts should be zero. However, since WCP are employed in the experiment, the histogram follows again a gaussian curve and is peaked at the same time bin as the two unfiltered histograms.

When HOM interference is measured with short pulses, it is possible to scan the coincidence curve as a function of the time delay between the two pulses. In this case, the 400ns-long pulses allow us to employ an alternative technique developed by [**?**], where the pulses are overlapped and the coincidence scan is performed between different time bins within the two detected single-photon histograms.

We fixed the time-bin j of one histogram, and scanned for coincidence counts in the second histogram. With this method, the two-photon coincidence histogram is still a gaussian, but it is possible to observe a superimposed HOM dip centered on the $j-th$ time bin. Without the j selection, the effect is averaged over all

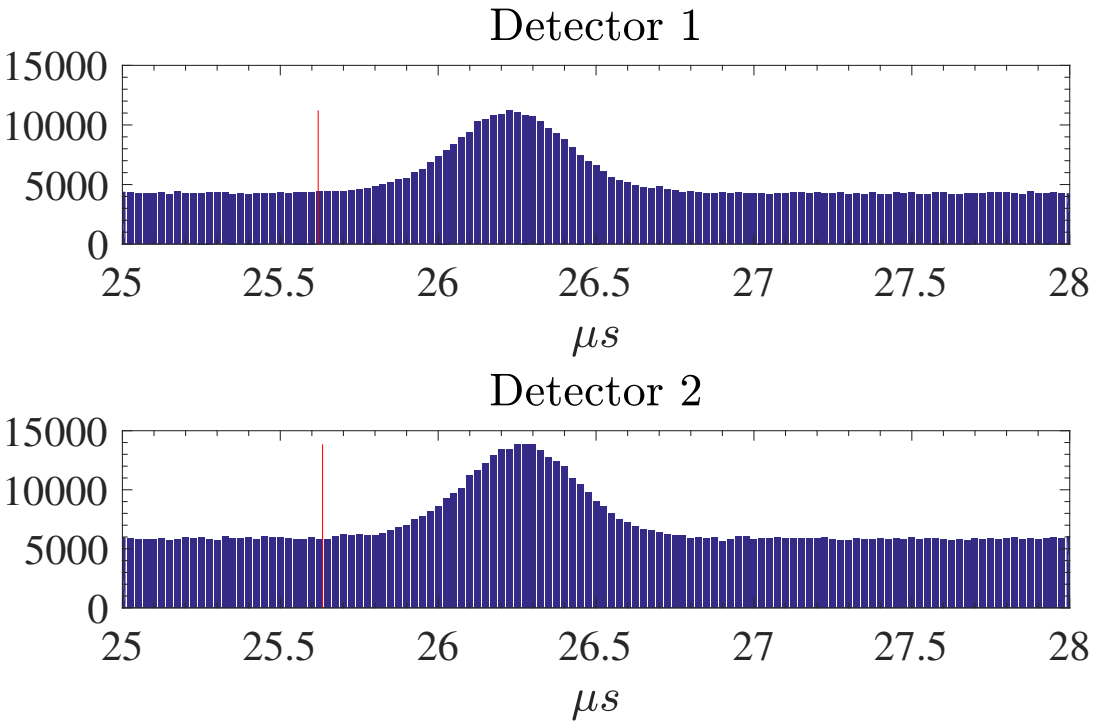


Figure 4.6: Histrogram with the unfiltered counts in detector 1 and 2.

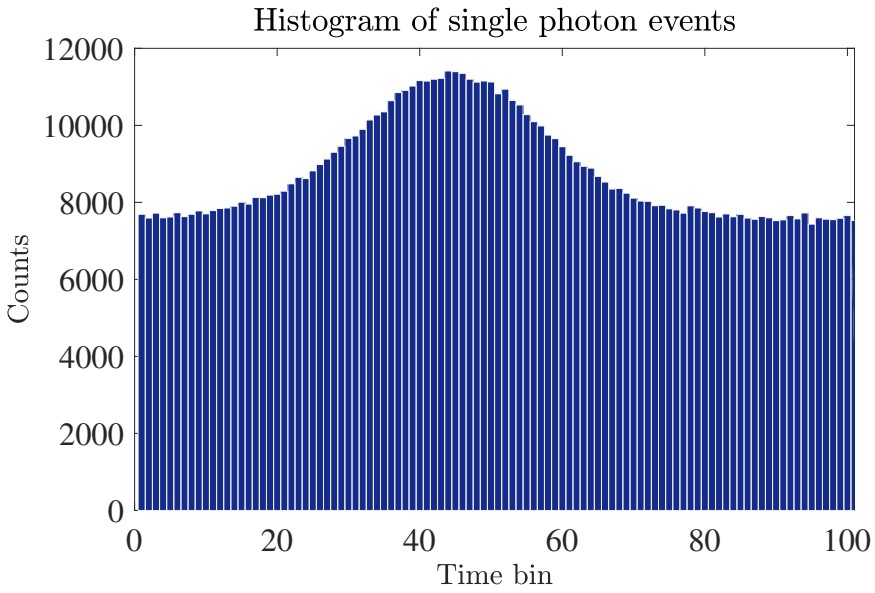


Figure 4.7: Filtered histogram corresponding single-photon counts for both detectors.

bins and the HOM is not observable.

The best visibility is in principle achieved by selecting a j time bin at the peak of the histogram, which in our case corresponds to bins 45 ± 1. Figure (4.8) shows the results of the bin selection and scanning.

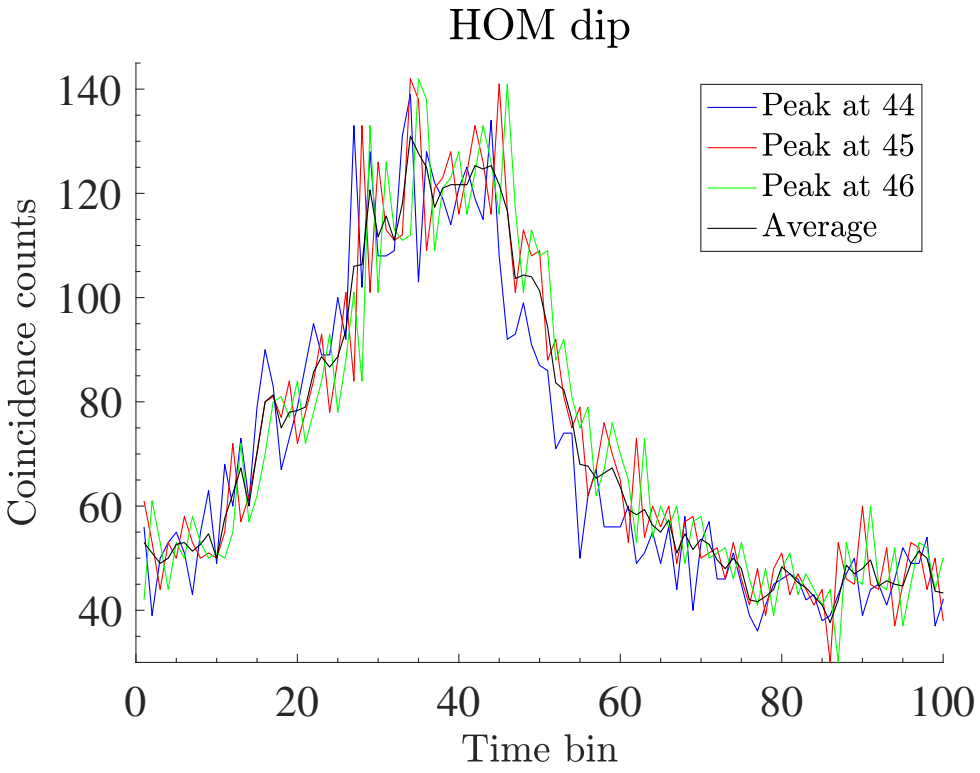


Figure 4.8: HOM dip for two-photon coincidences, filtered on time bins at the pulse peak

The measured visibility of the HOM dip is:

$$V_{HOM} = 12\% \tag{4.2}$$

Several factors contributed to reducing this value:

1. First of all, by using WCP the maximum achievable visibility is 50%.
2. The reflectivity of the 50:50 NPBS is optimised for a wavelength of 780nm, and at $\lambda = 795$nm the reflectivity was measured to be $R = 40 - 45\%$.
3. The most limiting factor is however the continuous background which affects the data. This background is independent of the environment and, as was realised after the experiment, appears to be generated by the AOMs.
   The power in the input branches of the interferometer was equalised while still observing the classical pulses and then attenuated at the main source, whose beam is then divided to become the input of Alice's and Bob's AOMs. The optical response of AOMs appears to depend on the input number of photons and for weak pulses interaction with the sound wave inside the AOM becomes a scattering process. The reduced efficiency of the AOM results in *CW leakage light* most likely constitutes the background in the data. By attenuating after the AOM the *CW leakage light* would probably be substantially reduced.
   An order of magnitude of this efficiency loss is given by the SNR of the pulse histograms, and is $36 - 42\%$.

In principle, all these effects have a multiplicative effect and the expected visibility is:

$$V_{HOM}^{theor} = 50\% \otimes 2R \otimes SNR = 16 - 18\% \tag{4.3}$$

which is coherent with what is observed in the experiment.

5

Storage and interference with quantum memory

After measuring the interference between the two pulses generated by the two sources, the setup was modified to include a quantum memory in the Alice channel, before the interferometer.

5.1 Storage of pulses in a room-temperature quantum memory

The 400-ns long pulses produced by Alice's AOM are +80MHz shifted with respect to the input laser and therefore the frequency lock of the control field has to be adjusted to compensate for this shift and maintain the condition on the two-photon detuning $\delta = 0$.

The storage was performed with classical pulses containing on average 10^8 photons, so that the SNR ratio between probe and control field is high enough that the control field can be filtered without requiring the etalon setup, and the 40dB provided by the output PBS are sufficient.

The adiabatic preparation of the atoms in the memory is achieved by varying the control field power. The processi is composed of three stages: writing, storage and retrieval.

Writing. When the pulse arrives at the memory the control field is high and the pulse is slowed down to the reduced group velocity v_g, that arises from EIT, and compressed in length to a factor of c/v_g. In the case of our room-temperature Rb-vapour quantum memory, $v_g \sim 10^5 m/s$ and for 400ns-long pulses the pulse length is compressed from $d = 120m$ to $d \sim 10cm$ which is comparable to the size of the Rb-vapour cell (5cm).

Storage Immediately after the pulse enters the memory, the control field is reduced to zero over a time interval of 10ns and as explained in Section (1.2.3) this creates a coherent transfer (mapping) of the amplitude from the probe

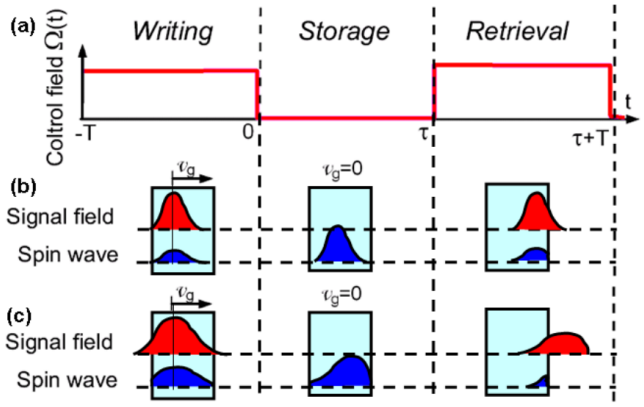


Figure 5.1: Cartoon representation of the storage process: (a) Time variation of the control field. (b) Storage under ideal conditions. (c) Realistic storage.

field to the collective spin excitation of the medium (the dark-state polariton). The amplitude of the spin excitation is proportional to the strength of the control field, as per Eq. (1.15). The storage time is limited by the lifetime of the dark-state polariton. In other words, atomic coherence is preserved in the medium until collisions and radiative decay prevail.

Retrieval The retrieval of the pulse is triggered by the control field. As the control is turned back on, the coherence is transferred back from the spin wave to the probe field.

Under realistic conditions, the group velocity may not be sufficiently reduced by EIT to compress the whole probe pulse inside the medium, so that the front of the pulse escapes the cell before control field is turned off. Accordingly, the tail of the pulse may not be stored since it does not enter the medium during the writing stage.
Moreover, the bandwidth of the pulse should match the bandwidth of EIT which is 1MHz.

Figure (5.2) shows the results obtained for the storage of pulses for intervals varied between 500ns and 2.9μs. The peak on the left represents the portion of the pulse which is slowed down but is unstored. The retrieved stored pulse is also truncated and the retrieval efficiency decays exponentially with increasing storage time. This degradation is caused by decoherence of the atomic excitations which result in a reduced optical depth. The coherence time of the quantum memory was estimated to be $\tau = 1\mu s$. The Rb-vapour quantum memories studied in this work have been proved to be able to preserve the coherence and store pulses for $\tau = 40\mu s$. The reason for the reduced coherence observed in this experiment is most likely due to non-perfect EIT conditions in the cell, particularly, residual magnetic fields and a non-uniform heating of the cell.

Temperature disomogeneities may cause the formation of rubidium condensation on the windows of the cell, which results in reduced visibility and efficiency.

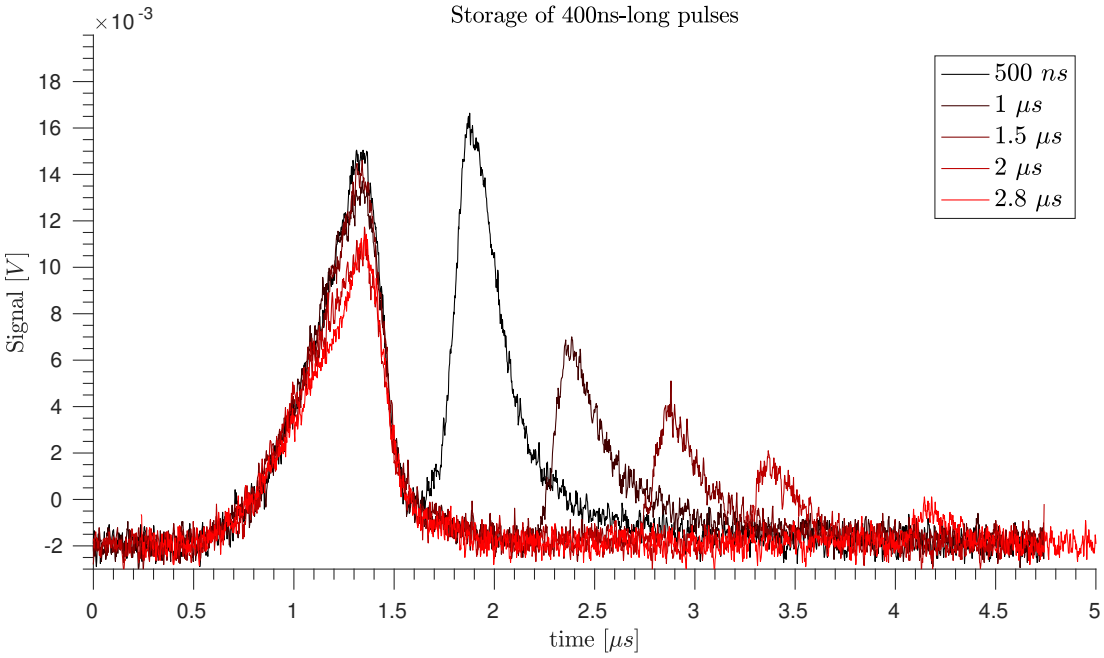


Figure 5.2: Retrieved pulse shape after different storage times. Decoherence causes an exponential decay of the storage efficiency.

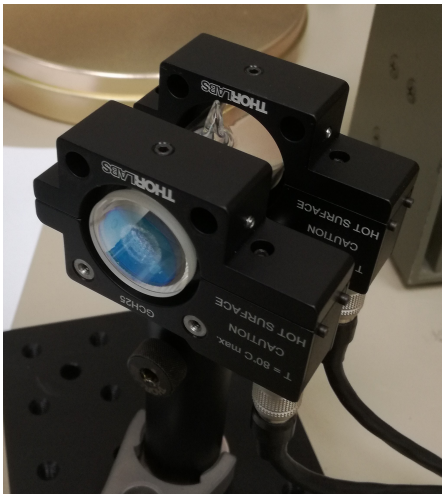


Figure 5.3: Picture showing the Rb condensation on the window of a vapour cell. In order to eliminate the condesation, the cell has to be removed from the quantum memory and placed on a special heater: repeated slow heating cycles at $70-80°C$ regenerate the cell and eliminate the condensation.

5.2 Pulse interference with a quantum memory

The first step towards realising MA-MDI-QKD is to demonstrate that it is possible to use the quantum memory in one channel to match for delays introduced in the other channel and measure interference between the stored pulse and the delayed pulse.

In the following experiment, one pulse was stored in the quantum memory, while the other was sent directly from the source to the interferometer. The unstored pulse was delayed and shifted in frequency to observe classical beat-note interference between the stored and unstored pulses.

Figure (5.5) shows the effect of the control field on the interference. Without

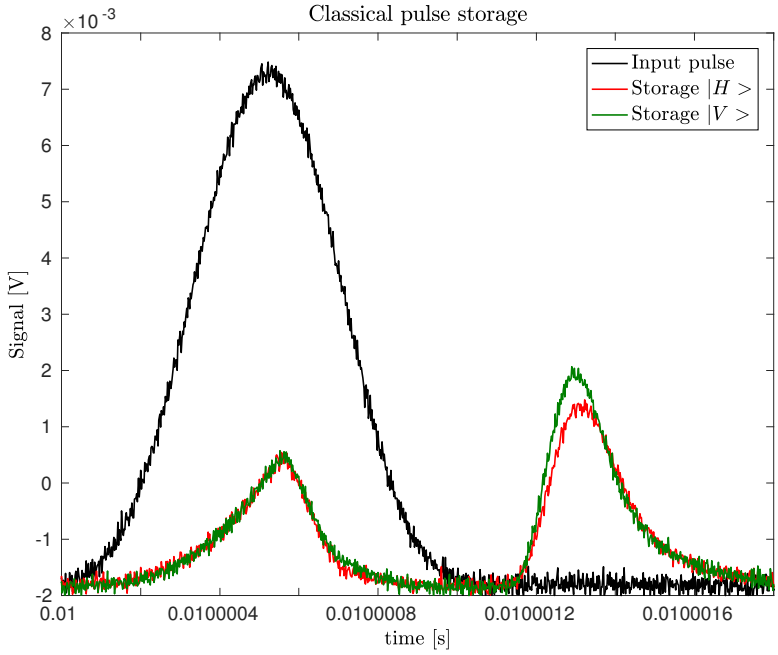


Figure 5.4: Storage of classical 400ns-long pulses for 10μs under optimal conditions: both polarisations are stored with the same efficiency

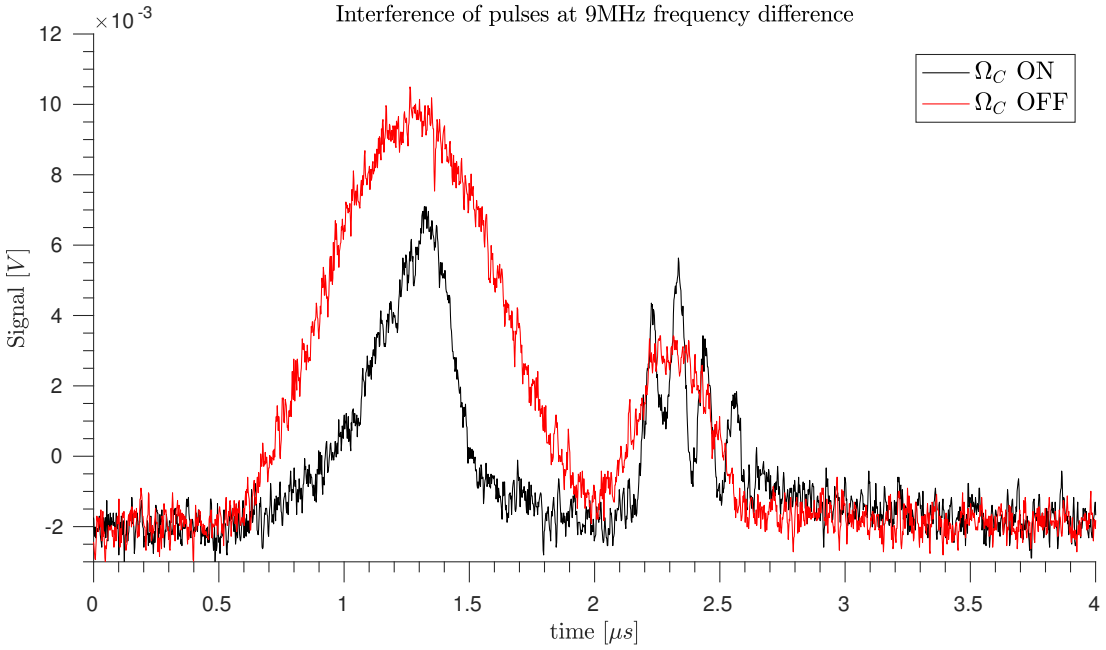


Figure 5.5: Interference of classical 400ns-long stored and delayed pulses, 9MHz-shifted in frequency, after storage for 1μs

EIT and modulation of the control field, the two pulses produced by the sources (in red in the graph), do not overlap and no interference can be observed. By modulating the control field, instead, it is possible to match the storage time of the memory to the 1μs delay introduced in the other channel and beat-note interference fringes appear. The same measurement was performed by varying the frequency difference and storage time and Figure (5.6) shows the result for a

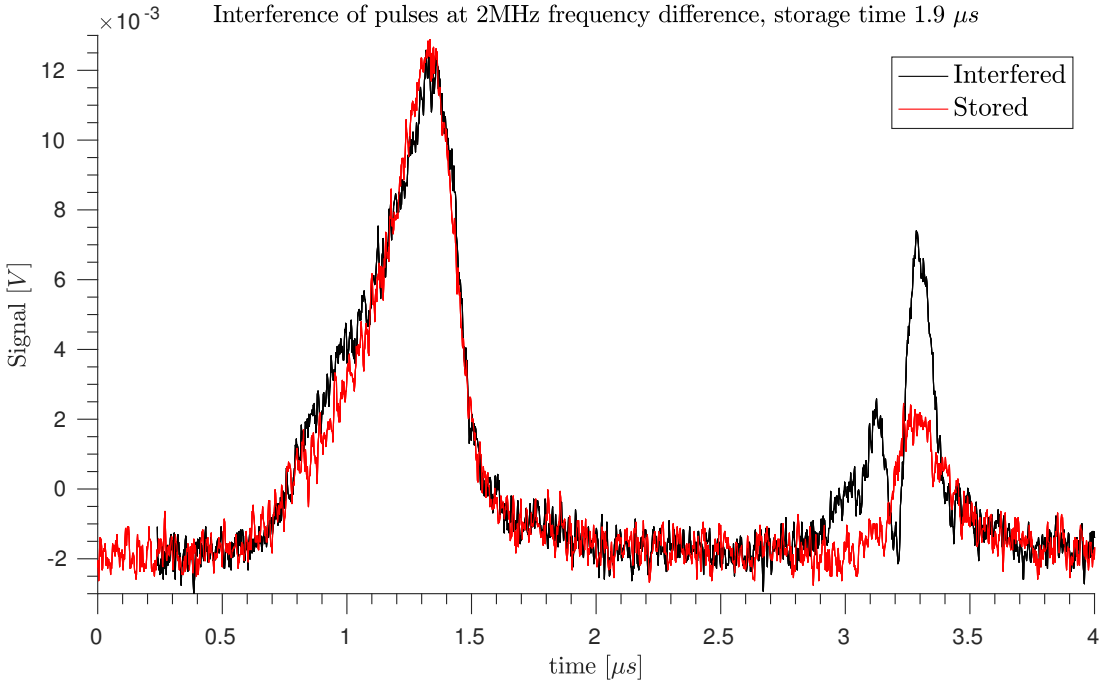


Figure 5.6: Interference of classical 400ns-long stored and delayed pulses after storage for 1.9μs

storage time of 1.9μs and frequency difference of 2MHz. Despite the weak signal, the interference still exhibits a visibility above 70%.

6 Setup for the random polarisation qubit source

In order to perform the storage and interference of pulses, the polarisation could be manually varied by applying the appropriate high voltage to the EOMs through a DC power supply and HV amplifier. For MDI-QKD applications, however, the twin sources' EOMs should be driven independently to produce a random polarisation modulation with a switching frequency equal to the repetition rate of the pulses produced by the AOMs.

In this Chapter, I will present the design and implementation of a high-voltage switching circuit, together with the development of the digital interface, implemented on an FPGA, which is needed to produce the triggers for the four voltage levels of the EOM driver, for the AOM and for the detectors.

6.1 Design and implementation of a driver circuit for the EOM

For BB84 qubits, the EOM driver needs to switch between four voltage levels in order to generate the states $\{|H\rangle, |A\rangle, |V\rangle, |D\rangle\}$. For an input $|H\rangle$ polarisation state and a wavelength of 795nm, these voltage levels become:

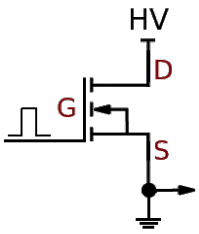
The optical pulses generated by the AOMs are gaussian, 400ns-long and have a repetition rate of 20kHz. For each period, the EOM driving signal should be a squared pulse synchronised with the AOM pulse. The duration, ripple, rising- and falling-time of the driving pulse should be optimised so that the polarisation is modulated uniformly for each optical pulse.

Polarisation	$\|H\rangle$	$\|A\rangle$	$\|V\rangle$	$\|D\rangle$
Voltage	0V	$\frac{1}{2}V_\pi = 131.6V$	$V_\pi = 263.2V$	$\frac{3}{2}V_\pi = 394.7V$

Table 6.1: EOM voltages and corresponding polarisation shifts

6.1.1 General idea of the design

From an electronic point of view, the EOM represents a capacitive load (C_{load}=14pF) driven by the driver's voltage and referenced to ground. Essentially, the high-voltage switch is implemented with a voltage-controlled n-channel high-voltage MOSFET.



- The drain (D) is connected to the HV rail
- The gate (G) is controlled by a logic signal, which will be the switch trigger produced by the FPGA.
- The source (S) is connected to the load and ground.
- When the input is "high" - above $V_{GS}^{(th)}$ - the switch is activated and current flows in the DS channel.

The design contains three high-voltage MOSFETs, whose drain terminals are connected to $V_{3\pi/2}$, V_{π} and $V_{\pi/2}$, respectively. The source terminals are isolated by high-voltage diodes and connected to the load. The gates of the three MOSFETs are driven by logic signals produced by the FPGA which at every period triggers one of the three channels, corresponding to a switch to polarisation $|D\rangle$, $|V\rangle$ or $|A\rangle$. The fourth state $|H\rangle$ simply corresponds to ground and is produced when all three channels are off.

The advantage of this configuration is that the switch is voltage-controlled and power is dissipated only during switching process. However, since the load is connected between S and GND, the switch is in a high-side configuration and direct logic drive is not possible. Given that in this design the source terminals swing from GND to HV, the gate voltage must be referenced to the source otherwise the threshold condition would never be satisfied. A gate driver is therefore needed between the MOSFET and digital input and a bootstrap circuit is necessary.

6.1.2 Bootstrap gate drive technique

In the bootstrap technique, a gate driver is accompanied by a bias circuit, both referenced to the source of the main MOSFET transistor so that both the driver and the bias circuit swing between the input high-voltage rail and ground together with the source of the device. However, the driver and its floating bias can be implemented by low voltage circuit elements since the input voltage is never applied across their components. The driver and the ground referenced control signal are linked by a level-shift circuit which must tolerate the high voltage difference and considerable capacitive switching currents.

A typical implementation representing the bootstrap technique is displayed in Figure (6.1). The level-shift circuit is comprised of a high-side gate driver, a bootstrap diode D_{BST}, a driver capacitor C_{DRV}, a high-voltage n-channel MOSFET, a bootstrap capacitor C_{BST} and a gate resistor R_{gate}.

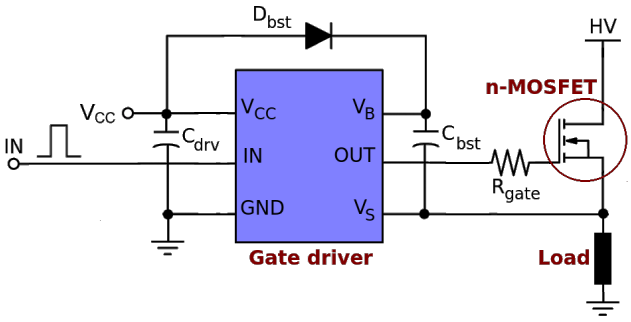


Figure 6.1: Typical scheme for n-MOSFET gate switching with bootstrap technique

The circuit operation is treated extensively in [13] and can be summarized as follows:

1. During the off time of the switch, C_{BST} is charged to the V_{CC} level through D_{BST}. This current is supplied by C_{DRV}.
2. When the logic input goes high to turn on the MOSFET, the gate charge necessary to establish the threshold voltage $V_{GS}^{(th)}$ is drawn from C_{BST}.
3. As the MOSFET turns on, its source swings to the positive input rail HV. D_{BST} blocks the input voltage and power to the driver is provided from the bootstrap capacitor.
4. At turn-off, the logic input goes low turning off the MOSFET. The voltage on the load swings back to ground.
5. As the gate of the MOSFET discharges, the drain-to-source voltage increases and the source transitions to ground, allowing D_{BST} to turn-on and the charging cycle for C_{BST} to restart.

6.1.3 Dimensioning and simulation

MOSFET. The maximum drain-source voltage of the MOSFET should be sufficient to stand the required high voltage. The on-state resistance of the channel $R_{DS}^{(on)}$ should be as low as possible so as to generate less heat. The MOSFET chosen is a TK31A60W with $V_{DS}^{(max)} = 600V$, $R_{DS}^{(on)} = 73m\Omega$, $V_{th} = 3.7V$, $t_{on} = 70ns$ and $t_{off} = 165ns$.

Gate driver. The selected component is a IR2117 high-side, high-speed non-inverting gate driver able to withstand an offset of the level-shift circuit up to 600V. The driver can source and sink $I = 290 - 600mA$ with a turn-on and turn-off time of 230ns. The input logic level *high* of the IR2117 is 9.5V and the driver cannot be interfaced direcly with the logic signals from the FPGA.

Bootstrap capacitor. The value of the bootstrap capacitor is crucial in detemining the maximum *on* time of the switch. The value of C_{BST} must be at

least:

$$C_{BST} = \frac{Q_{CB}}{\Delta V_{CB}} = \frac{Q_G + t_o n \cdot I_B}{\Delta V_{CB}} \tag{6.1}$$

where $I_B = 400\mu$A is the supply bias current of the IR2117 and$\Delta V_{CB} = 1\%V_{CC} = 0.15$V is the maximum allowable voltage ripple. For $t_{on} = 2\mu$s $C_{BST} \gtrsim 700n$ and a value $C_{BST} = 1\mu$F as chosen.

Driver capacitor. As a rule of thumb, the driver capacitor must satisfy $C_{DRV} \sim 10 \cdot C_{BST}$ and $C_{DRV} = 10\mu$F.

Gate resistor. The purpose of the gate resisitor is to dampen any oscillations in the output of the gate driver. The optimal value was calculated to be $R_{gate} = 62\Omega$.

Bootstrap and output diodes. The voltage rating of D_{BST} and D_{OUT} must be sufficiently high to stand-off the high-side MOSFET drain voltage and a current rating greater than or equal to the maximum average current at switching. It must also have a sufficiently fast reverse-recovery time to avoid momentarily sourcing current from the high-voltage drain supply into the lower voltage V_{CC} supply.

Pull-down resistor. A 10Ω resistor is placed between the output to the EOM and ground to create a discharge path for the EOM when all switches are off.

HV DC-DC converter The high-voltage is supplied by a DC-DC converter, which for ann input voltage of 12V produces an output voltage of 500V,which is then divided to produce $V_{3\pi/2}$, V_π and $V_{\pi/2}$. The output current of 20mA is not sufficient for switching the load, therefore a 1μF storage capacitor is placed between each drain and ground and acts a charge reservoir for switching.

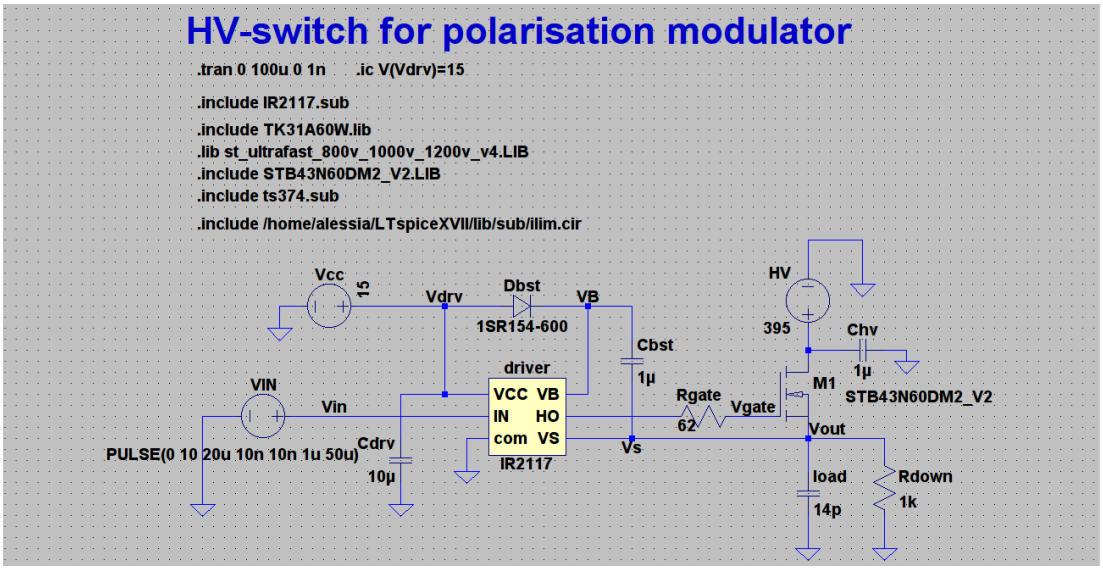
Figure (6.2) shows the results of the design and simulation of the individual switch.

The circuit was realised on a two-layer PCB, whose design is shown in Figure (6.4) and (6.5).

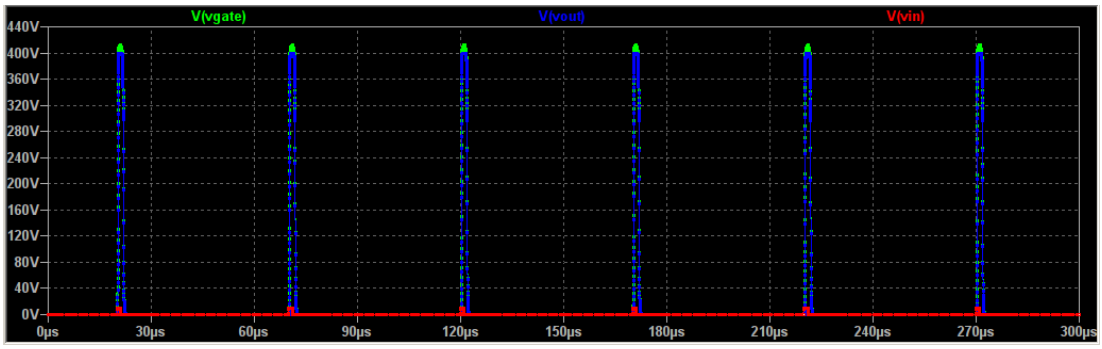
6.2 Electronic control of the setup via FPGA

For both Alice and Bob, the FPGA digital interface controls the triggering of one of the four BB84 polarisation states produced by the driver, the triggering of the AOM which produces the pulse and the triggering of the detectors.

The chip employed is a Zedboard. The device was programmed using the Xilinx Vivado suite and VHDL hardware programming language. The design is essentially composed of three logic modules per source: a block memory generator, a pulse-shaping block and an EOM switching block. All signals are timed with a 100MHz Clock and the design also includes an asynchronous Reset.



(a) Circuit schematic of one of the three parallel switches.



(b) Simulated square pulses: input $V_{IN} = 10V$ (red), MOSFET gate signal $V_{gate} = HV + V_{cc}$ (green) and output signal $V_{out} = HV$ (blue).

Figure 6.2: Schematic and simulation results of one of the three switches.

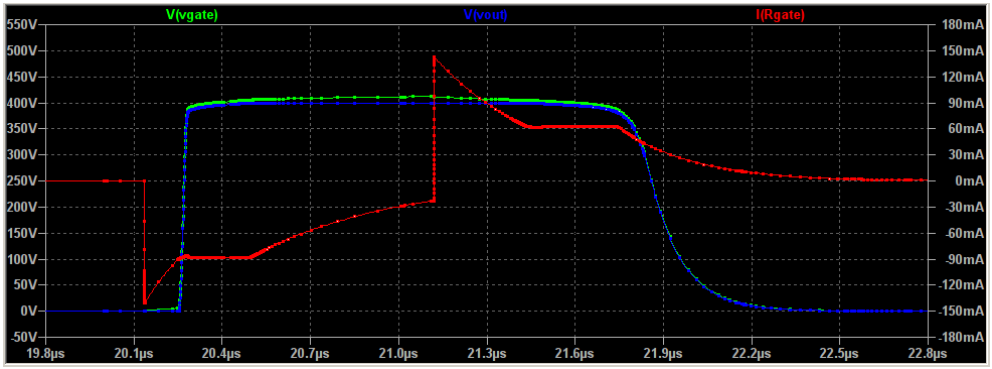


Figure 6.3: Output pulse signal V_{out} (blue), gate signal V_{gate} (green) and gate current I_{Rgate} (red). The simulation shows that the current sourced and sunk by the gate driver ($\pm$150mA) is within the operational limits of the IR2117.

Pulse-shaping block. The digital interface is designed to operate at a switching frequency of 20kHz, so the role of the first block is to reshape the clock and

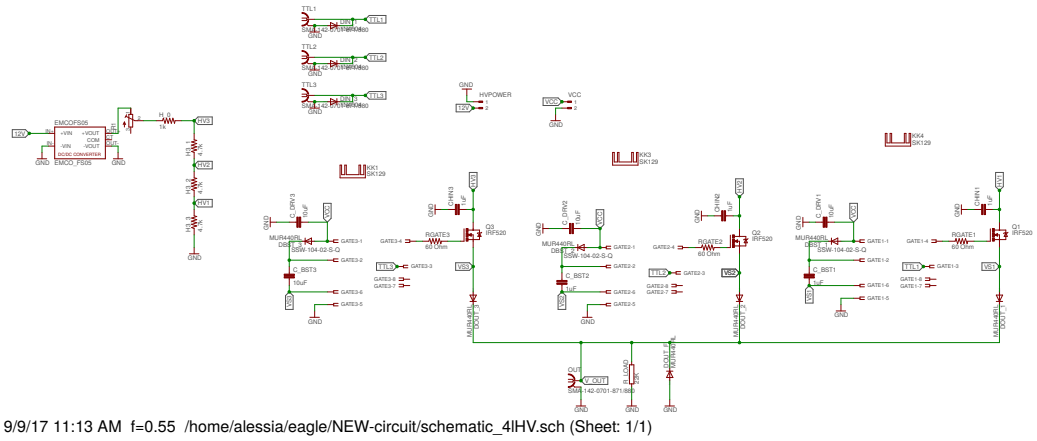


Figure 6.4: Complete circuit schematic

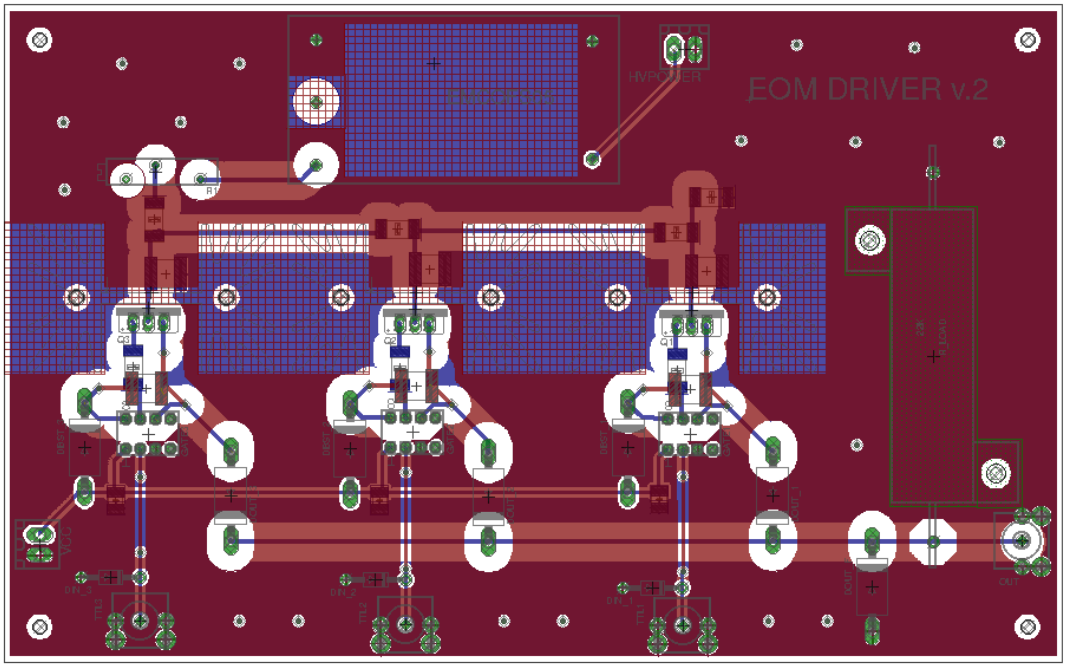


Figure 6.5: PCB layout: top layer (red) and bottom layer (blue)

produce the triggering signals for the update of the memory address NEXT-ADDRESS, the enabling of the switching and the AOM and detector trigger.

Block memory generator. The two memory blocks are loaded with two coefficient files which contain two binary random sequences. The address is updated at the beginning of each $50\mu s$ cycle of the switch and the *word* read from the memory is teo-bits long. The output of the memory is then fed to the EOM-switching block.

EOM switching block. The EOM block produces the signals that are used as inputs for the four-level switch circuit. At the beginning of each switch cycle, the block receives a two-bit long logic vector read from the memory.

Depending on the value of the *word* the block outputs a logic signal in one of the four output ports which is synchronised with the enable signal from the pulse-shaping block.

Input word	{00}	{01}	{10}	{11}
Output singnal channel	$\|H\rangle$	$\|A\rangle$	$\|V\rangle$	$\|D\rangle$

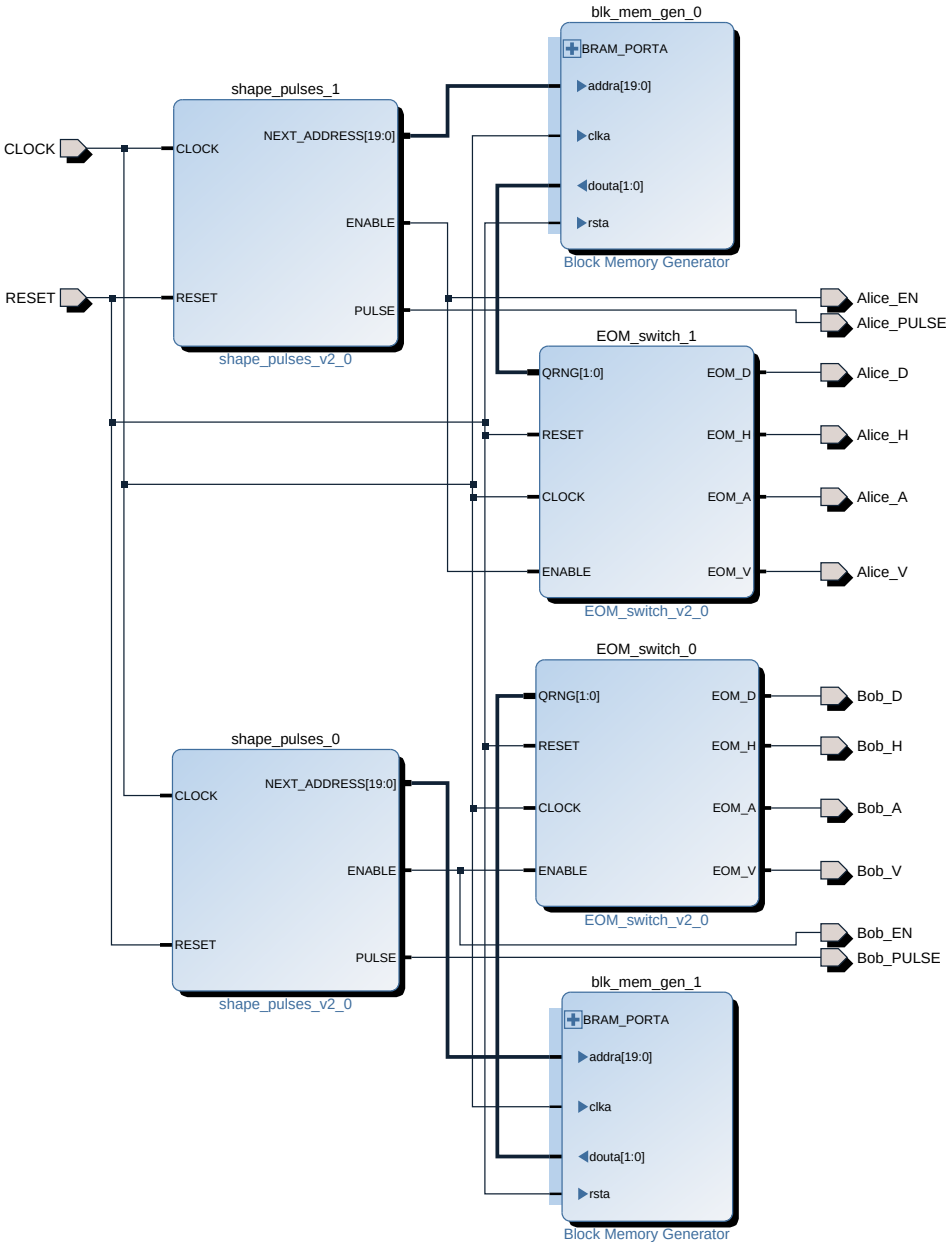


Figure 6.6: Design schematic of the FPGA digital interface

7 Summary and outlook

7.1 Summary

- In this thesis, I described the theory and operation of Rb-vapour room-temperature quantum memories and their applications in quantum communication.
- I set up two twin polarisation qubit sources which employ acousto-optic modulators (AOMs) for pulsing and electro-optic modulators (EOMs) for polarisation switching.
- I set up an interferometer to measure both classical and quantum interference.
- I observed classical beat-note interference both with continuous waves and pulses.
- I measured Hong-Ou-Mandel two-photon interference between two weak coherent pulses produced by the sources, observing a HOM dip visibility of 12%.
- I measured the characteristics of pulses stored in the quantum memory, particularly varying the storage time between $500ns - 2.8\mu$s.
- I measured classical interference between a pulse stored in a quantum memory and a pulse delayed at the source.
- I designed a 4-level high-voltage switch to be used as a driver for the EOMs, and programmed an FPGA to be used as a digital interface for the two drivers, the two AOMs and the detection setup.
- As a preliminary work, I studied and measured the propagation properties of vortex beams carrying orbital angular momentum produced by q-plates, their intensity distribution and wavefront.

7.2 Outlook

The results presented in this thesis are a first step towards the integration of a Rb-vapour room-temperature quantum memory in a measurement-device-independent quantum key-distribution scheme to perform MA-MDI-QKD.

The QuantumFuture group in Padova and the QIT group in Stony Brook plan to extend the collaboration, and I will continue working on this project as a PhD student in the QuantumFuture group.

In this respect, this thesis is a work-in-progress and many improvements and upgrades are possible and planned.

- A second quantum memory will be implemented in the channel which, for this first experiment, was only delayed, so as to achieve fine control on the overlap of the pulses and timing of the interference.
- The coherence (i.e. storage) time of the quantum memories is considerably improved by using paraffin-coated cells, where the dephasing due to collisions is reduced.
- Two extra detectors will be added to the interference setup to perform a complete Bell-state measurement.
- Once the setup is optimised for single-photon operation, a crucial experiment before the realisation of MA-MDI-QKD will be HOM interference with two quantum memories.
- As for the random qubit sources needed for the QKD experiment, the custom high-voltage electronics designed for driving the EOMs is delicate and cannot handle switching frequencies higher that 30kHz. A more robust solution, yet more expensive, would be to design a custom low-voltage switch, and interface it with a high-voltage amplifier to achieve the correct driving voltages for the EOM.

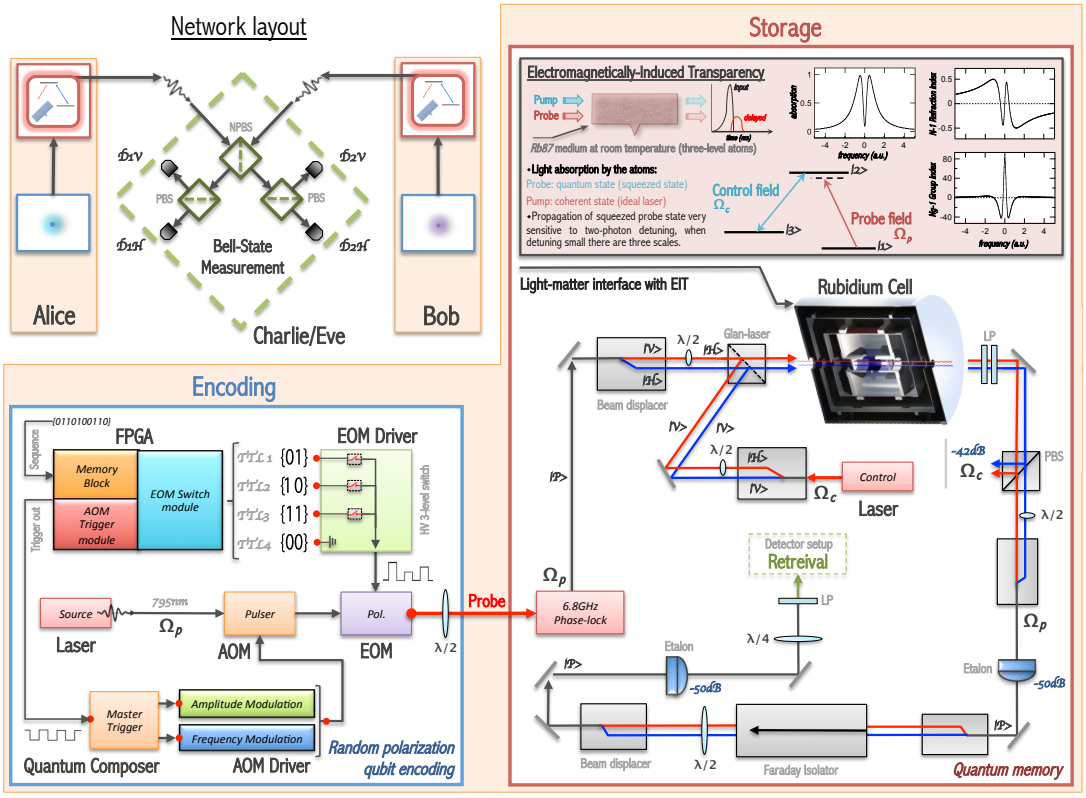


Figure 7.1: Upgrade of the experiement to perform MA-MDI-QKD

A

Study of orbital angular momentum states

A.1 OAM states for Quantum Communication

Orbital angular momentum (OAM), together with spin angular momentum (SAM), is an intrinsic property of light. From a classical point of view, in the paraxial limit the two components can be readily associated to different properties of the optical beam: the SAM is associated with the beam's circular polarization content while the OAM is associated with the helical structure of the optical wavefront around the beam axis and with an optical vortex located on the beam axis.

The main motivation for the study of OAM states for quantum information and quantum communication applications arises from the fact that the OAM value is independent of the choice of coordinates and therefore, unlike polarisation encoding, transmitter and receiver are not required to precisely align their references. Moreover, whereas the photon's SAM can only take two values, $S_z = \pm\hbar$, the value of OAM per photon can assume any integer value multiple of $\hbar$:

$$L_z = \pm m\hbar \tag{A.1}$$

The OAM unit m also defines the phase variation of the wavefront, described by the m-fold helix $exp(im\varphi)$, where φ is the azimuthal angle in the plane orthogonal to the propagation axis. This higher dimensionality of the OAM states allows to encode information in qudits, i.e., qubits of dimension d.

OAM states have already been used to realise free-space QKD links [14], but unfortunately, due to their higher divergence, the maximum distance of the channel is constrained to a few km. As explained in Section **??**, it is also more difficult to correct any aberrations and distortions induced on the wavefront of an OAM beam by atmospheric turbulence.

An interesting perspective would open from the study of the storage of OAM states in a quantum memory. As explained in the following section, OAM beams can be produced by conversion from SAM states, in a process called spin-to-orbital-conversion (STOC). This transformation is unitary and can therefore be reversed to re-obtain a SAM state with a fidelity as high as 98% [15].

If indeed OAM states and their superpositions are preserved after propagation in the medium and can be stored in a room-temperature atomic-vapour quantum memory, this might allow a qubit-storage scheme alternative to the dual-rail operation where the polarisation qubit is transformed in a superposition of OAM states in a STOC process, and after retrieval from the quantum memory the STOC is reversed to re-obtain a SAM state.

As a preliminary work, I studied and measured the propagation of OAM beams generated by a q-plate.

A.2 Generation of OAM states with q-plates

q-plates are birefringent liquid crystal waveplates that exploit STOC to convert a polarisation state into an orbital state. Specifically, q-plates induce a uniform phase delay δ and orientation of the optical axis α that follows a pattern which is a function of the polar coordinates in the transverse plane.

$$\alpha = f(\rho, \varphi) \tag{A.2}$$

The pattern exhibits a topological singularity of charge $q = \frac{|l|}{2}$ at the plate center. In the formalism of Jones' matrices, the transformation of the beam throught the q-plate is described by:

$$T(\rho, \varphi) = \cos\frac{\delta}{2}\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix} + i\sin\frac{\delta}{2}\begin{bmatrix}0 & e^{-2if(\rho,\varphi)}\\ e^{2if(\rho,\varphi)} & 0\end{bmatrix} \tag{A.3}$$

For optimal tuning conditions $\delta = \pi$ the STOC efficienty is 100% and for an input $l = 0$ circularly polarised beam, the q-plate produces output with OAM content $l = 2q$ and inverted handedness of the polarization.

A.2.1 Alignment and tuning of the q-plate

The STOC conversion efficiency is enhanced by properly aligning the beam with the q-plate and maximising the beam radius, so as to make the beam interact with a larger area of the q-plate. It is also crucial that the beam be a TEM_{00} Gaussian mode.

The input laser beam at $\lambda = 850nm$ was elliptic and affected by aberrations. After coupling into a single-mode optical fiber, the output is filtered to produce a Gaussian beam and by finely adjusting the position of an aspheric lens with focal length $f = 18.4mm$ placed at the output of the fiber it was possible to produce a collimated beam with the waist W_0 at the q-plate position. The beam

Waist radius	$W_0 = (1.580 \pm 0.002)mm$
Rayleigh range	$z_0 = (9.227 \pm 0.028)m$
Waist position	$z = 27mm$

polarisation was converted to circular with a polariser and quarter-waveplate $\lambda/4$ at 45°: the relative visibility variation measured is $\sim 3\%$.

The alignment of the center of the q-plate with the axis of the beam was performed by observing the q-plate output when placed between two orthogonal polarisers.

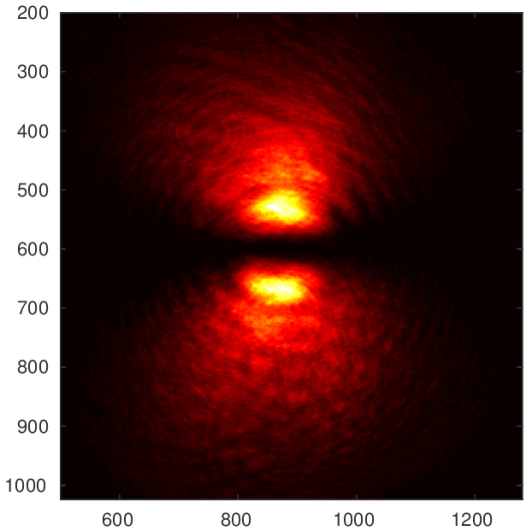


Figure A.1: q-plate between cross polarisers.

The q-plate can be finely tuned by applying a RF voltage modulation, without which the output state would be a superposition of the converted and unconverted beam:

$$|0, R\rangle \rightarrow cos(\delta/2)\,|l, L\rangle + sin(\delta/2)\,|0, R\rangle \tag{A.4}$$

The optimal tuning condition ($\delta = 0$) was found by transforming beam polarization back to linear with $\lambda/4$ plate at 45° and introducing a PBS to separate the $|V\rangle$ unconverted component from the $|H\rangle$ OAM component. With the optimal modulation, the power measured in the unconverted branch vanishes. The optimal modulation was found to be a $2kHz$ sinewave with an amplitude of $V = 1.982V$.

A.3 Circular beams and their properties

The intensity distribution of optical beams produced with a q-plate is not simply described by Laguerre-Gauss beams, but is a more complex Circular Beam (CiB).

$$CiB_{p,l}^{\xi,q_0}(r,\phi) = \mathcal{N}\left(1+\xi\frac{q_0^*}{q_0}\right)^{\frac{p}{2}}\left(i\frac{r\sqrt{kz_0}}{q_0}\right)^{|l|} G(r)\,{}_1F_1\left(-\frac{p}{2}, |l|+1; \frac{r^2}{\chi^2}\right) e^{il\phi} \tag{A.5}$$

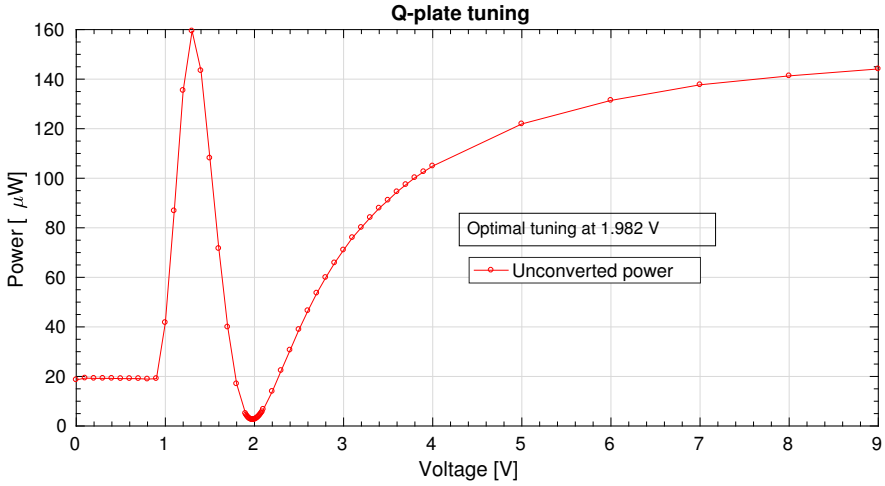


Figure A.2: Unconverted power as a function of the voltage applied to the q-plate: the minimum corresponds to the optimal tuning.

where $G(r)$ is the underlying Gaussian beam, ${}_aF_b$ is the Generalised Hypergeometric Function and $\mathcal{N}$ is a normalisation factor.

$$G(r) = \frac{i}{q_0}\sqrt{\frac{kz_0}{\pi}}e^{-\frac{ikr^2}{2q_0}} \tag{A.6}$$

$$\mathcal{N} = |l|!{}_2F_1\left(-\frac{p}{2}, -\frac{p^*}{2}, |l|+1, |\xi|^2\right)^{-1/2} \tag{A.7}$$

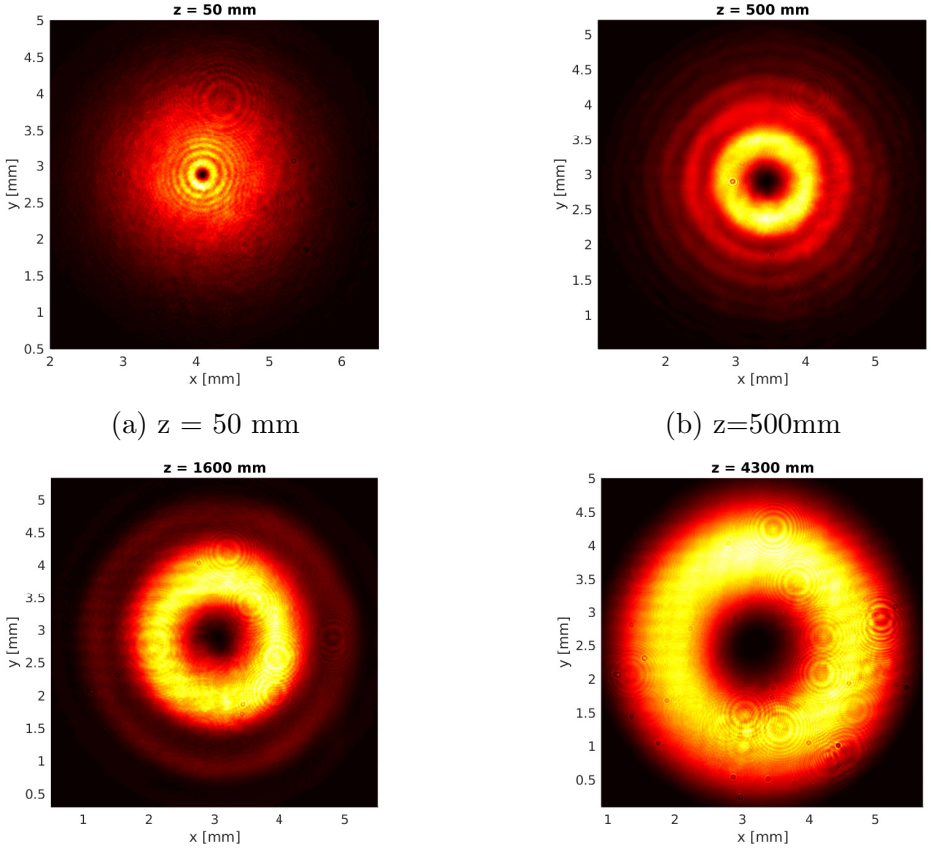
$$\frac{1}{\chi^2} = \frac{kz_0\xi}{q_0}\frac{1}{q_0 + \xi q_0^*} \tag{A.8}$$

With q-plate placed at the Gaussian beam waist: $(\Delta \to 0)$

- $\xi = \frac{z_0 - i\Delta}{z_0 + i\Delta} = 1$
- ξ is invariant under propagation.
- $p = -|l|$

A.3.1 Radial intensity profile of vortex beams

Figure (A.3) shows the vortex beam intensity profile for different distances from the q-plate. The radial symmetry of the profile was exploited to more efficiently analyse its properties and reduce noise: the profiles were averaged over concentric rings centered on the beam axis and compared to the prediction of the CiB model.



(a) z = 50 mm (b) z=500mm

(c) z=1600mm (d) z=4300mm

Figure A.3: Intensity distribution of vortex beams at different distances

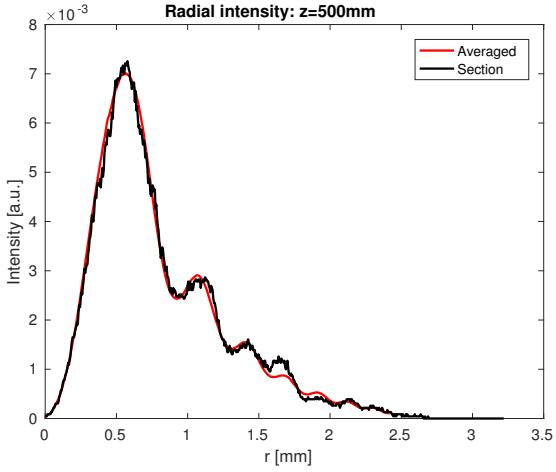


Figure A.4: Comparison of cut and averaged profiles at z=500mm

A.3.2 Expansion in Laguerre-Gauss modes

The CiB beam solution can be written as a weighted superposition of an infinite number of Laguerre-Gauss modes.

$$CiB_{p,l}^{(\xi,q_0)} = \sum_{n=0}^{+\infty} C_n LG_{n,l}^{(q_0)} \tag{A.9}$$

where the coefficients C_n in the case studied where $\xi = 1$, $p = -|l| = -1$ are given by:

$$C_n = C_0 \frac{1}{\sqrt{2n!}} = \frac{1}{\sqrt{{}_2F_1\left[\frac{1}{2}, \frac{1}{2}, 2, 1\right]}} \cdot \frac{1}{\sqrt{2n!}} \tag{A.10}$$

It has been demostrated in [16] that the CiB solution can also be expressed in a form for which the expansion is optimised, i.e., it allows the series truncation at lower values of n. This is achieved by shifting the beam parameter q_0 of the Laguerre-Gauss mode in the right-hand side of the expansion to:

$$q_0' = -d_0 + i\gamma_{opt} z_0 \tag{A.11}$$

where $\gamma_{opt} = 1/2$ for $l = 1$, $\xi = 1$, $p = -1$.

$$CiB_{p,l}^{(\xi,q_0)} = \sum_{n=0}^{+\infty} C_n' LG_{n,l}^{(q_0')} \tag{A.12}$$

The new coefficients are given by:

$$C_n' = C_0' \frac{1}{\sqrt{2n!}} = 2\left(\frac{2}{3}\right)^{3/2} C_0 \tag{A.13}$$

The experimental data was compared to the LG and opt-LG expansion models. The data shows good with the CiB model. The root-mean-square-error (RMSE) quantifies the deviation of the two approximations from the CiB solution. The RMSE decreases increasing the number of modes considered in the expansion and indeed the optimised expansion converges to the CiB solution much faster, allowing a reduction of a factor of 10^2 on the number of modes to be included in the series in order to obrain the same RMSE. Furthermore, increasing the distance, fewer LG modes are needed to obtain a good approximation which signifies that the CiB solution evolves towards a pure Laguerre-Gauss mode in the far field.

A.3.3 Vortex radius, encircled-energy radius and divergence

The most striking difference between LG and CiB beams is that the former are modes, while the latter are not. This becomes clear when we examine the vortex size, defined as the distance from the beam axis at which the intensity is $1/e^2$ the peak intensity in the main ring. Indeed, the vortex size of LG modes is fixed along the propagation, while for CiB modes it evolves and grows as $R_V \propto \sqrt{z}$.

The enclosed-energy radius R_{EE} is defined as the radius of the circle that contains a fraction $E_0 = 1 - 1/e^2$ of the total beam energy. A theorem on the divergence

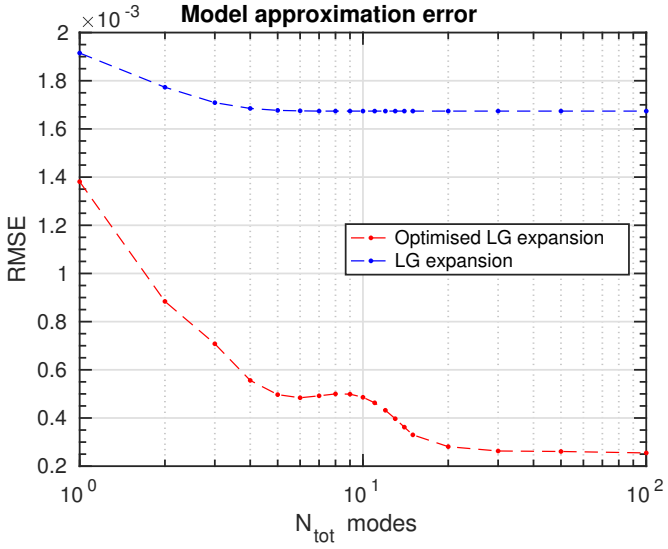


Figure A.5: Convergence of the LG and opt-LG models as a function of the number of modes

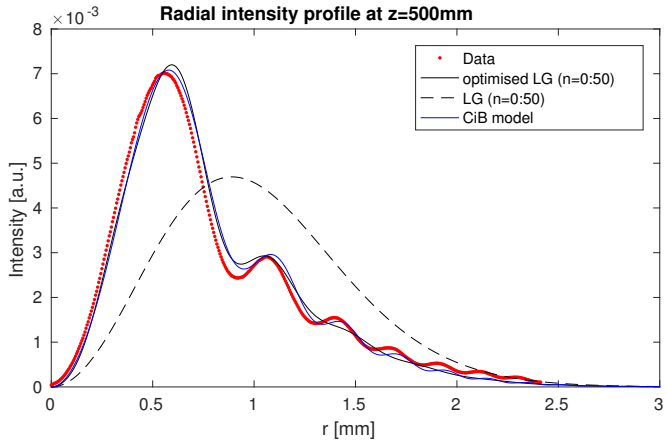


Figure A.6: Convergence of the models for z=500m, n=50 modes

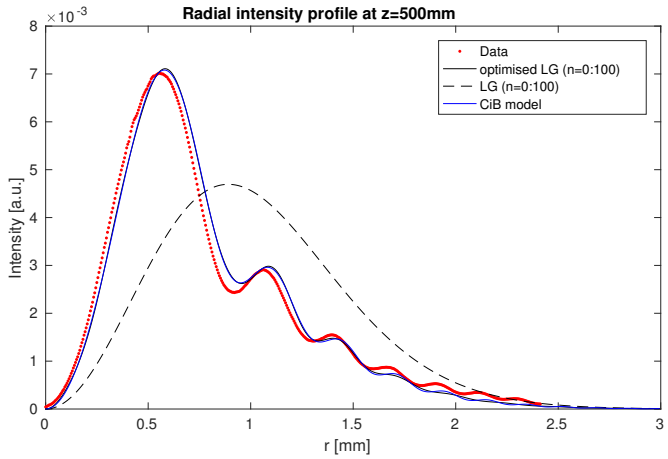


Figure A.7: Convergence of the models for z=500m, n=100 modes

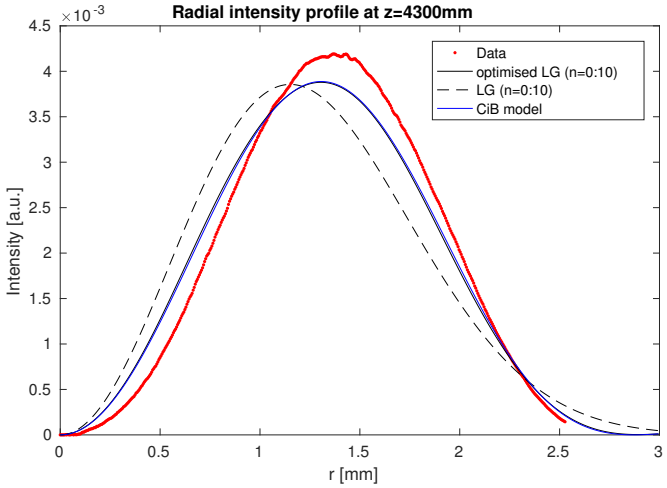


Figure A.8: Convergence of the models for z=4300m, n=10 modes

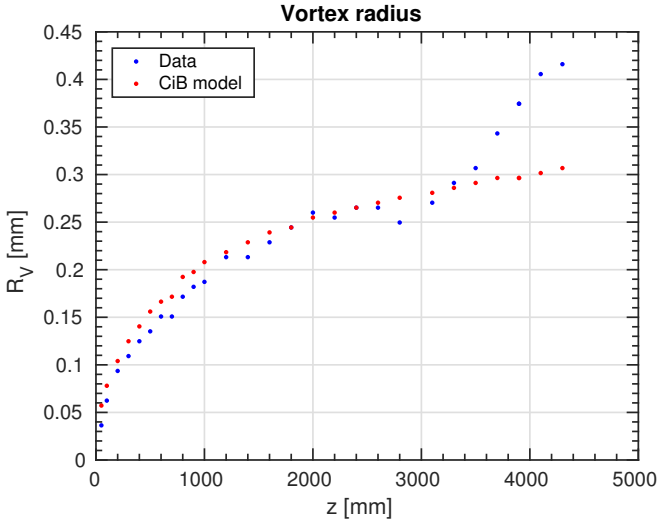


Figure A.9: Vortex radius as a function of the distance from the q-plate.

of Vortex beams [17] predicts:

$$\vartheta_{EE} = \lim_{z \to +\infty} \frac{R_{EE}(z)}{z} \tag{A.14}$$

$$\tag{A.15}$$

$$\mathbb{M}^2 = \frac{2\pi}{\lambda} \vartheta_{EE} min(R_{EE}) \tag{A.16}$$

$$\geq 1.8 + |l| \tag{A.17}$$

The divergence was measured to be $\vartheta_{EE} = 4 \cdot 10^{-4}$ while the beam-quality factor is $\mathbb{M}^2 = 3.99 > 2.8$.

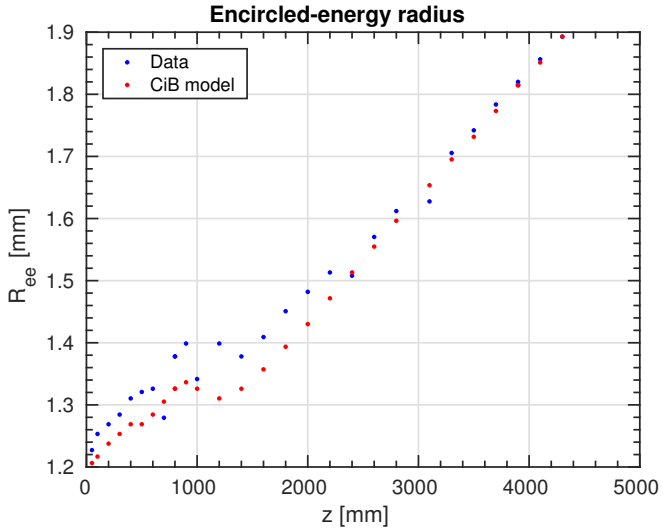


Figure A.10: Enclosed-energy radius as a function of the distance from the q-plate

A.3.4 Imaging of the q-plate: Vortex closure

An optical imaging system was set up to measure the precise evolution of the vortex size immediately after the q-plate. At the q-plate position, the vortex is a phase singularity on the axis of a gaussian beam. The setup is composed of two lenses: the 1st lens $f_1 = 50mm$ is placed at distance $d_1 = f_1$ from q-plate, while the 2nd lens $f_2 = 200mm$ is placed at distance $d_2 = f_1 + f_2$ from 1st lens, so as to create a real image of the q-plate at a distance $d_3 = f_2$ from the 2nd lens. The value of the focal length of the two lenses was chosen to achieve the largest magnification possible and increase the resolution on the vortex size. The minimum vortex diameter observed was rescaled to account for the magnification factor of the optical imaging system and was calculated to be $R_V = 2 \pm 1\mu m$, which is below the pixel dimension of $4.7\mu m$ of the sensor employed which would be the limiting parameter without magnification.

A.4 OAM beam wavefront

The amplitude of an OAM beam $\mathbb{LG}_l(\rho)$ is a superposition of Laguerre polynomials. The wavefront is an l -fold helix, hence an on-axis phase discontinuity arises.

$$\Psi_l(\rho, \phi) = \mathbb{LG}_l(\rho) e^{il\phi}$$

A.4.1 Zernike Polynomials

A generic wavefront can be decomposed in a series of (orthogonal) Zernike polynomials $Z_n^m(\rho, \vartheta)$ with each term corresponding to a particular physical aberration

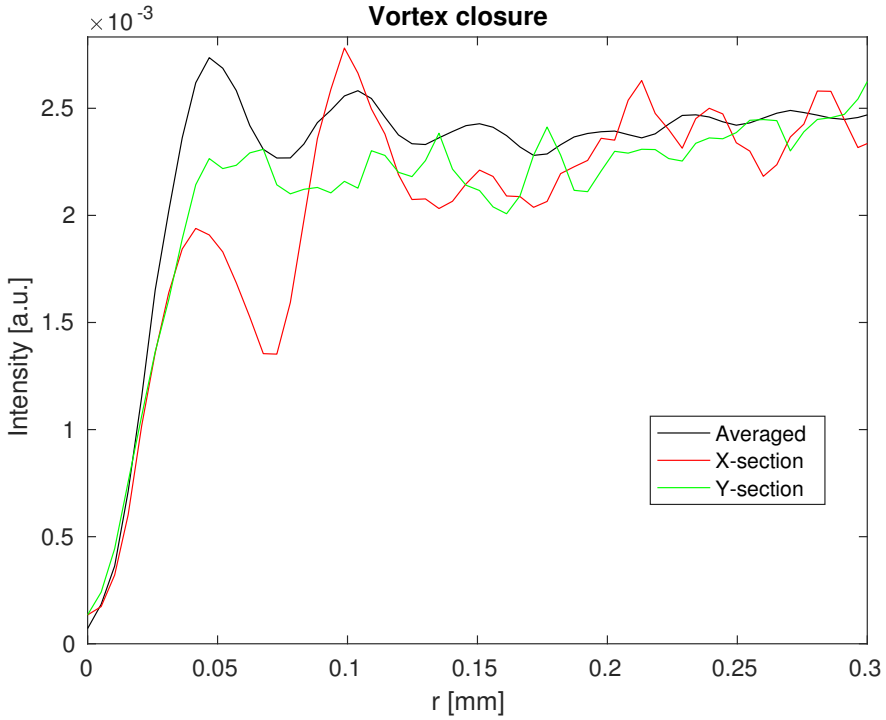


Figure A.11: a

affecting the wavefront.

$$W(\rho,\vartheta) = \sum_{n,m} c_n^m Z_n^m(\rho,\vartheta) \tag{A.18}$$

Zernike polynomials

$$\begin{cases} Z_n^m(\rho,\vartheta) = N_n^m R_n^{|m|}(\rho)\cos(m\vartheta) & for\ m \geq 0 \\ Z_n^m(\rho,\vartheta) = -N_n^m R_n^{|m|}(\rho)\sin(m\vartheta) & for\ m < 0 \end{cases}$$

where $N_n^m\sqrt{\frac{2(n+1)}{1+\delta_{m0}}}$, $n \in \mathbb{N}$ and $m = \{-n, -n+2, -n+4, \ldots, n-2, n\}$.

$R_n^{|m|}(\rho)$ is the radial Zernike polynomial defined as:

$$R_n^{|m|}(\rho) = \sum_{s=0}^{(n-|m|)/2} \frac{(-1)^s(n-s)!}{s![0.5(n+|m|)-s]![0.5(n-|m|)-s]!}\rho^{n-2s} \tag{A.19}$$

In the case of an OAM beam, the decomposition in Zernike terms requires an infinite amount of Zernike terms in order to completely reconstruct the OAM wavefront. However, it can be demonstrated that a pure OAM state has zero projection on any Z_n^m mode if m=0 and from this [3] derived a hybrid basis to decompose the wavefront of an OAM beam.

Indeed, since radial Zernikes Z_n^0 are orthogonal to OAM modes, this means that radial aberrations do not affect the OAM content of the beam. Conversely, azimuthal Zernikes Z_n^m are not orthogonal to OAM modes. and this means that

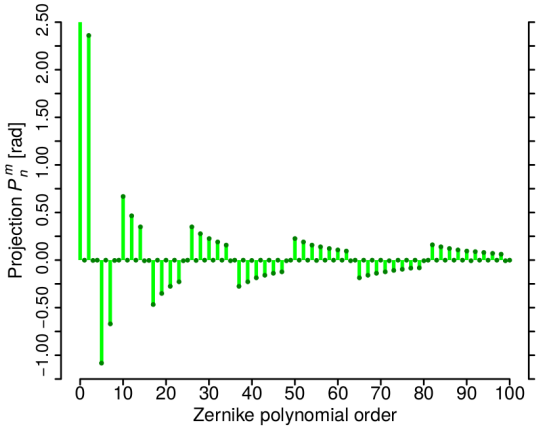


Figure A.12: From [3]: Zernike projection of vortex $l = 1$. The piston term $n = 0$, not shown completely, is equal to $\pi^{3/2}$.

azimuthal aberrations can be mistakenly identified even for a pure unaberrated OAM beam and conversely, azimuthal aberrations do affect the OAM content of the beam, corresponding to a broadening of the OAM spectrum. Therefore, Azimuthal Zernikes and OAM modes are a basis for the same subspace.

In the "hybrid" OAM-Zernike basis, the radial Zernikes and OAM modes can be combined to form a complete orthogonal alternative basis [3] and describe the OAM beam wavefront in presence of generic aberrations and/or a superposition of different OAM states.

$$\Psi(\rho,\phi) = \mathbb{LG}(\rho) \cdot e^{i\left[\sum_{n,Even} c_n R_n^0(\rho)\right]} \cdot \sum_l d_l e^{il\phi - i\phi_l} \tag{A.20}$$

A possible application of this hybrid basis would be in the detection of OAM states with a Shack-Hartmann wavefront sensor. By implement the new basis in the modal reconstruction of the wavefront from the sensor's data it would be readily possible to identify the OAM spectrum.

The wavefront can be explicitly written as:

$$W(\rho,\phi) = arg\left[\Psi(\rho,\phi)\right] = \arctan\left[\frac{\sin\left(\sum_n b_n R_n^0(\rho)\right) + \sum_l d_l \sin\left(l\phi - \phi_l\right)}{\cos\left(\sum_n b_n R_n^0(\rho)\right) + \sum_l d_l \cos\left(l\phi - \phi_l\right)}\right] \tag{A.21}$$

Which can be approximated as follows in the case of a superposition of unaberrated OAM states.

$$W(\rho,\phi) = \arctan\left[\frac{\sum_l d_l \sin(l\phi - \phi_l)}{\sum_l d_l \cos(l\phi - \phi_l)}\right] \tag{A.22}$$

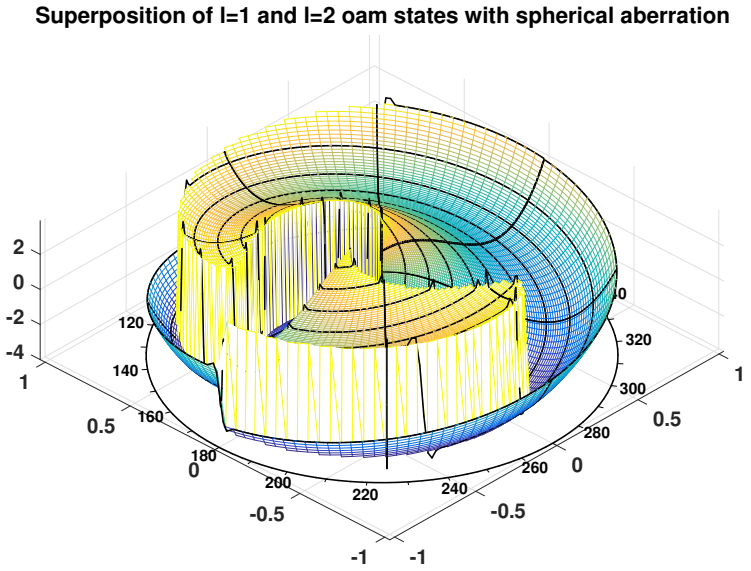


Figure A.13: Wavefront for a superposition of OAM states $l = 1$ and $l = 2$.

Instead, for a pure OAM state affected by aberrations $Z = \sum_n b_n R_n^0(\rho)$:

$$W(\rho,\phi) = \arctan\left[\frac{\sin(Z)+\sin(l\phi-\phi_l)}{\cos(Z)+cos(l\phi-\phi_l)}\right]$$
$$= \arctan\left[\frac{2\sin\left(\frac{Z+l\phi-\phi_l}{2}\right)\cos\left(\frac{Z-l\phi+\phi_l}{2}\right)}{2\cos\left(\frac{Z+l\phi-\phi_l}{2}\right)\cos\left(\frac{Z-l\phi+\phi_l}{2}\right)}\right] = \frac{\sum_n b_n R_n^0(\rho)+l\phi-\phi_l}{2}$$

Bibliography

[1] M. Fleischhauer and M. D. Lukin, "Dark-State Polaritons in Electromagnetically Induced Transparency," *Phys. Rev.Lett.*, vol. 84, no. 22, 2000.

[2] M. Namazi, G. Vallone, B. Jordaan, C. Goham, R. Shahrokhshahi, P. Villoresi, and E. Figueroa, "Free space quantum communication with quantum memory," *preprint available at arXiv:1609.08676*, 2016.

[3] N. Uribe-Patarroyo, A. Alvarez-Herrero, and T. Belenguer, "A comprehensive approach to deal with instrumental optical aberrations effects in high-accuracy photon's orbital angular momentum spectrum measurements," *Optics Express*, vol. 18, no. 20, p. 21111, 2010.

[4] I. Damgård, S. Fehr, L. Salvail, and C. Schaffner, "Secure identification and QKD in the bounded-quantum-storage model," *Theoretical Computer Science*, vol. 560, no. P1, pp. 12–26, 2014.

[5] A. K. Ekert, "Quantum Cryptography Based on Bell's Theorem," *Phys. Rev.Lett.*, vol. 67, no. 6, pp. 661–663, 1991.

[6] H.-k. Lo, M. Curty, and B. Qi, "Measurement-Device-Independent Quantum Key Distribution," vol. 130503, no. March, pp. 1–5, 2012.

[7] S. Harris, "Eletromagnetically Induced Transparency," *Physics Today*, pp. 36–42, 1997.

[8] G. Brennen, E. Giacobino, and C. Simon, "Focus on Quantum Memory," *New Journal of Physics*, vol. 17, 2015.

[9] C. Simon, M. Afzelius, Appel, *et al.*, "Quantum memories :A review based on the European integrated project"Qubit Applications (QAP)"," *European Physical Journal D*, vol. 58, no. 1, pp. 1–22, 2010.

[10] M. Namazi, C. Kupchak, B. Jordaan, R. Shahrokhshahi, and E. Figueroa, "Unconditional polarization qubit quantum memory at room temperature," pp. 1–6, 2015.

[11] C. K. Hong, Z. Y. Ou, and L. Mandel, "Measurement of Subpicosecond Time Intervals Between Two Photo By Interference," *Phys. Rev.Lett.*, vol. 59, no. 18, pp. 2044–2046, 1987.

[12] J. Jin, J. A. Slater, E. Saglamyurek, N. Sinclair, M. George, R. Ricken, D. Oblak, W. Sohler, and W. Tittel, "Two-photon interference of weak coherent laser pulses recalled from separate solid-state quantum memories," *Nature Communications*, vol. 4, pp. 1–7, 2013.

[13] Balogh Laszlo, "Design And Application Guide For High Speed MOSFET Gate Drive Circuits," tech. rep., 1998.

[14] G. Vallone, V. D'Ambrosio, A. Sponselli, S. Slussarenko, L. Marrucci, F. Sciarrino, and P. Villoresi, "Free-space quantum key distribution by rotation-invariant twisted photons," *Physical Review Letters*, vol. 113, no. 6, pp. 1–8, 2014.

[15] L. Marrucci, E. Karimi, S. Slussarenko, B. Piccirillo, E. Santamato, E. Nagali, and F. Sciarrino, "Spin-to-orbital conversion of the angular momentum of light and its classical and quantum applications," *Journal of Optics*, vol. 13, no. 6, p. 064001, 2011.

[16] G. Vallone, "Role of beam waist in Laguerre – Gauss expansion of vortex beams," *Optics Letters*, vol. 42, no. 6, pp. 1097–1100, 2017.

[17] G. Vallone, "On the properties of circular beams: normalization, Laguerre–Gauss expansion, and free-space divergence," *Optics Letters*, vol. 40, no. 8, p. 1717, 2015.

[18] N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, "Device-Independent Security of Quantum Cryptography against Collective Attacks," *Phys. Rev.Lett.*, vol. 98, no. June, pp. 1–4, 2007.

[19] N. L. Piparo, N. Sinclair, and M. Razavi, "Memory-assisted quantum key distribution resilient against multiple-excitation effects," vol. 1, 2017.

[20] N. Gisin and R. Thew, "Quantum Communication," *Nature Photonics*, vol. 1, 2007.

[21] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Reviews of Modern Physics*, vol. 74, no. 1, pp. 145–195, 2002.

[22] R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek, B. Ömer, M. Fürst, M. Meyenburg, J. Rarity, Z. Sodnik, C. Barbieri, H. Weinfurter, and A. Zeilinger, "Entanglement-based quantum communication over 144km," *Nature Physics*, vol. 3, no. 7, pp. 481–486, 2007.

[23] Z. Tang, Z. Liao, F. Xu, B. Qi, L. Qian, and H.-K. Lo, "Experimental Demonstration of Polarization Encoding Measurement-Device-Independent Quantum Key Distribution," *Physical Review Letters*, vol. 112, no. 19, p. 190503, 2014.

[24] I. Novikova, R. Walsworth, and Y. Xiao, "EIT-based slow and stored light in warm atoms," *Laser & Photonics Reviews*, no. July, pp. 1–21, 2011.

[25] M. Fleischhauer and J. Marangos, "Electromagnetically induced transparency : Optics in coherent media," *Reviews of Modern Physics*, vol. 77, no. April, pp. 633–673, 2005.

[26] C. Kupchak, T. Mittiga, B. Jordaan, M. Namazi, C. Nölleke, and E. Figueroa, "Room-Temperature Single-photon level Memory for Polarization States," *Scientific Reports*, vol. 5, p. 7658, 2015.

[27] M. Namazi, T. Mittiga, C. Kupchak, and E. Figueroa, "Cascading Quantum Light-Matter Interfaces," *Phys. Rev. A*, vol. 92, 2015.

[28] K. Boller, A. Imamolu, and S. Harris, "Observation of electromagnetically induced transparency," *Physical Review Letters*, vol. 66, no. 20, pp. 2593–2596, 1991.

[29] W. W. Erickson, *Electromagnetically Induced Transparency.* PhD thesis, 2012.

[30] H. Chen, X.-B. An, J. Wu, Z.-Q. Yin, S. Wang, W. Chen, and Z.-F. Han, "Hong–Ou–Mandel interference with two independent weak coherent states," *Chinese Physics B*, vol. 25, no. 2, p. 020305, 2016.

[31] P. Marek, P. Zapletal, R. Filip, Y. Hashimoto, T. Toyama, J.-i. Yoshikawa, K. Makino, and A. Furusawa, "Direct observation of phase sensitive Hong-Ou-Mandel interference," 2017.

[32] T. Wilk, *Quantum Interface between an Atom and a Photon.* PhD thesis, 2008.

[33] Y. S. Kim, O. Slattery, P. S. Kuo, and X. Tang, "Conditions for two-photon interference with coherent pulses," *Physical Review A - Atomic, Molecular, and Optical Physics*, vol. 87, no. 6, pp. 1–5, 2013.

[34] G. Vallone, G. Parisi, F. Spinello, E. Mari, F. Tamburini, and P. Villoresi, "General theorem on the divergence of vortex beams," *Physical Review A*, vol. 94, no. 2, pp. 1–8, 2016.

[35] B. Piccirillo, V. D'Ambrosio, S. Slussarenko, L. Marrucci, and E. Santamato, "Photon spin-to-orbital angular momentum conversion via an electrically tunable q -plate," *Applied Physics Letters*, vol. 97, no. 24, pp. 4085–4090, 2010.

[36] B. Piccirillo, V. Kumar, L. Marrucci, and E. Santamato, "Pancharatnam-Berry phase optical elements for generation and control of complex light: generalized superelliptical q-plates," *Spie Opto*, vol. 9379, p. 937907, 2015.

[37] N. Uribe-Patarroyo, A. Alvarez-Herrero, and T. Belenguer, "Measurement of the quantum superposition state of an imaging ensemble of photons prepared in orbital angular momentum states using a phase-diversity method," *Physical Review A - Atomic, Molecular, and Optical Physics*, vol. 81, 2010.

[38] F. a. Starikov, G. G. Kochemasov, S. M. Kulikov, a. N. Manachinsky, N. V. Maslov, a. V. Ogorodnikov, S. a. Sukharev, V. P. Aksenov, I. V. Izmailov, F. Y. Kanev, V. V. Atuchin, and I. S. Soldatenkov, "Wavefront reconstruction of an optical vortex by a Hartmann-Shack sensor.," *Optics letters*, vol. 32, no. 16, pp. 2291–3, 2007.

[39] L. Seifert, H. J. Tiziani, and W. Osten, "Wavefront reconstruction with the adaptive Shack-Hartmann sensor," *Optics Communications*, vol. 245, no. 1-6, pp. 255–269, 2005.

[40] M. Nielsen and I. Chuang, *Quantum Computation and Quantum Information*. Cambridge UP, 2010.

[41] U. Leohnhardt, *Measuring the Quantum State of Light*. Cambridge UP, 1997.

[42] V. Vedral, *Introduction to Quantum Information Science*. Oxford UP, 2006.

[43] B. Saleh and M. Teich, *Fundamentals of Photonics*. Wiley, 2007.