Characterization and demonstration of integrated ring resonator tPUKs

Master Thesis

L. van der Hoeven

Graduation committee:
Prof. Dr. P.W.H. Pinkse (AQO)
Dr. D.P. Stellinga (AQO)
Dr. Ir. J.S. Kanger
M.C. Velsink, MSc.

Applied Physics
Adaptive Quantum Optics
Faculty of Science and Technology
University of Twente
The Netherlands

May 2021

Abstract

As part of the search for powerful post-quantum cryptography methods, new security schemes have been put forward that rely on physical principles to withstand a quantum computer attack. These schemes utilize the properties of time-domain unclonable keys (tPUKs), in combination with temporal wavefront shaping. tPUKs are physical objects that possess an optical response that is hard to replicate using another device. Additionally, creating a functional copy of a tPUK is assumed to be infeasible due to manufacturing errors. In recent research, tPUK candidates such as multimode fibers have been characterized and have been demonstrated to work with temporal wavefront shaping. To overcome the shortcomings found for these candidates, such as input coupling dependence and bending instabilities, new integrated photonic chip tPUK designs, based on systems of ring resonators, were designed and fabricated.

The integrated tPUK samples are systems consisting of serially joined unit cells. These unit cells are made up of two waveguides, coupled by two ring resonators. We describe the integrated tPUK samples' transmission using a transmission matrix approach. To study the fabricated tPUK samples' unclonability and optical response, we experimentally measure their transmission properties and compare them to those predicted by the theoretical model. From these comparisons, we are able to verify that the fabricated tPUK samples mostly display the designed tPUK-like transmission characteristics. Additionally, we are also able to verify that the physical properties of the fabricated tPUK samples match those with which they were designed, apart from one parameter. Having characterized the tPUK samples, the theoretical model is adapted to a new promising unit cell design. Using the theoretical model we show that this new unit cell design can reduce tPUK system transmission losses and improve tPUK functionality in future generations of integrated tPUKs.

As a final experimental endeavor of the work presented in this thesis, we perform temporal wavefront shaping on the pulsed input of the fabricated tPUK samples to provide a demonstration of their tPUK functionality. The goal of the demonstration is to maximize the ratio between the non-linear intensities at the two spatial outputs of the tPUK samples. tPUK functionality is demonstrated for a system consisting of 13 ring resonator unit cells, where an output non-linear intensity ratio of factor 3 is reached.

Contents

1. Introduction

Throughout history, cryptography has played an essential role in providing secure communication [1]. The importance of this security has been made even more apparent with the comparatively recent introduction of the internet. Long-distance secure communication between parties is typically achieved by the exchange of secret keys. These shared secret keys are in essence series of bits that can be used to encrypt and decrypt messages or information. With recent advancements in the development of quantum computers and the ever-increasing computational power of classical computers the degree to which these security methods are deemed future proof has come into question. Commonly used and well-known cryptography methods such as RSA, elliptic curve cryptography (ECC), and Diffie–Hellman key exchange have been proven to be insecure against quantum computer attacks using Shor's algorithm [2–4]. Even though modern standardized symmetric encryption schemes such as AES are not directly broken by Shor's algorithm, their security is still greatly diminished by other future quantum possibilities such as Grover's algorithm [5, 6]. To address these concerns, multiple new post-quantum cryptography schemes have been proposed. The first proposed and arguably most well-known quantum cryptography protocol was a quantum key distribution (QKD) protocol presented by C. Bennet and G. Brassard in 1984 [7]. In this scheme, a quantum channel is used to exchange a secret key. Although this scheme protects against eavesdropping on the key exchange, it still requires an authenticated and thus secure classical communication channel for the duration of the key exchange to also be secure against impersonation attacks [8].

To provide authenticated channels as well as ensure secure communication a physical cryptography method has been proposed that relies on the use of physical unclonable keys (PUKs). In recent years optical approaches to such methods have been explored at the University of Twente [9, 10]. An example of an optical PUK would be a scattering medium. Such a medium scatters incoming light into a random-looking yet deterministic speckle pattern. Using wavefront shaping, one is able to spatially shape the phase of an input wavefront in such a way that where normally a speckle pattern would be observed, instead light is collected into a focus. This input wavefront is unique to the specific PUK as any other scattering medium will produce a speckle pattern. In this sense, the PUK acts as a unique key. It would be infeasible to make a copy of the PUK since the scattering is very sensitive to the positions of all the individual scatterers present in the scattering medium. To create a functional copy of the PUK one would need to replicate the entire PUK with an accuracy in the order of a few nanometers. This is impossible for modern fabrication methods [9, 11].

A proposed secure asymmetric communication method involving a PUK would have the party receiving a signal (Bob) in the possession of a PUK. The party sending a message (Alice) would send their message encoded into a wavefront that when received by Bob will produce a focus at one of two locations behind the PUK, representing either a 0 or a 1. To protect against eavesdroppers (Eve) Alice has to send her information in spatially shaped wavefronts that consist of fewer photons than the number of spatial shaping modes used. This communication method, called PUK enabled asymmetric communication (PEAC) [11], is secure because Alice is now ensured that only the intended receiver in possession of the PUK (Bob) can read her message. A noteworthy drawback of the PEAC scheme is that it works in the spatial domain and thus involves spatially shaped wavefronts. Diffraction

makes long-distance transmission of such wavefronts difficult in free space. Transmitting these wavefronts through optical fibers is also considered impractical due to the unstable characteristics of multi-mode fibers.

Fortunately, schemes such as PEAC can be adapted to work in the time domain. time-domain PEAC (tPEAC) makes use of a time-domain PUK (tPUK) that scrambles a single spatial input in time. Again a correct input will produce a focus in one of two spatial positions. The key difference is that these foci are made in time instead of in space. A time concentrated output will only be created if the optical pulse used as input possesses a time structure specific to the tPUK. Long distance transmission of such time-structured pulses is possible with low-loss single-mode optical fibers as they lack intermodal dispersion [12].

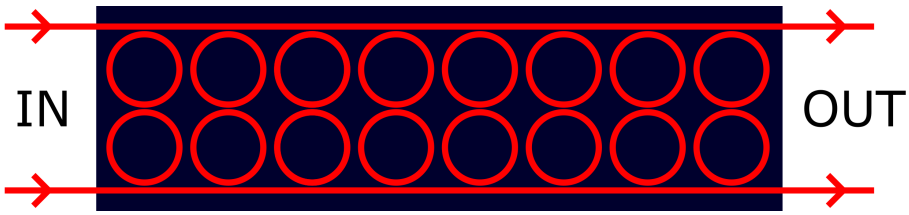

Figure 1.1: A sketch of an integrated ring resonator tPUK design.

Recent efforts in the AQO have been concerned with studying tPUK candidates suitable for security applications such as tPEAC. An example of such candidates is a Multimode fiber (MMFs). The limitations observed for MMFs sparked interest in tPUK candidates with true single spatial mode inputs that are also robust against environmental conditions [10]. To that end, photonic chips consisting of ring resonator structures have been put forward as promising tPUK candidates. Such photonic chips have also been fabricated. See figure 1.1 for a sketch of such a device. The main goal of the research presented in this thesis is to characterize the produced photonic chips and utilize temporal wavefront shaping to provide a proof of concept demonstration of their suitability in a security scheme such as tPEAC.

1.1 Outline

The next chapter, chapter 2, will provide the theoretical background for tPUKs, tPUKs consisting of ring resonator systems, temporal wavefront shaping, and security schemes involving tPUKs, such as tPEAC. Chapter 3 will elaborate on the integrated tPUKs that were studied for this thesis. Theoretical simulations are compared to experimental results and future design suggestions are made. Chapter 4 will give an overview of the experimental setup used to both study and demonstrate the integrated tPUKs. Chapter 5 presents a demonstration of the photonic chips' tPUK functionality. Chapter 6 discusses the experimental challenges encountered during this research. Chapter 7 provides a conclusion to this thesis and also presents interesting future research opportunities.

2. Theory

This chapter aims to explain the main theoretical concepts that are fundamental for understanding the results and conclusions presented in this thesis. First of all, a brief theoretical overview of tPUKs and their uses is given. In particular, the subject of a tPUK consisting of a ring resonator system is thoroughly covered. Secondly, the theory of wavefront shaping is elaborated upon. Lastly, the theory behind tPUK security schemes is covered, in which the earlier discussed theoretical topics are combined.

2.1 Time-domain physical unclonable keys

A physical unclonable key or function (PUK/PUF) is a physical object that transforms an incoming signal in a manner that is unique but also difficult to invert. The uniqueness of this transformation is guaranteed by the condition that it is infeasible to fabricate an object that features the same transformation as the original PUK [13]. An example of a PUK typically used in optics would be a scattering medium. Light from a coherent source will be transmitted and reflected by the scattering medium, producing speckle patterns in both cases. See the top part of figure 2.1 for an illustration. The specific characteristics of the observed speckle patterns depend on the numerous phase shifts encountered during propagation through the medium caused by individual particles of the scattering medium. To obtain a scattering medium that produces speckle patterns with the same characteristics, a copy has to be made that contains scattering particles on positions that are practically identical to the original medium. Even if the positions of all the original scattering particles are known any attempt at copying them is assumed to be infeasible in practice. Manufacturing limits are considered to be the main reason that copying a PUK is infeasible [9, 11, 13, 14].

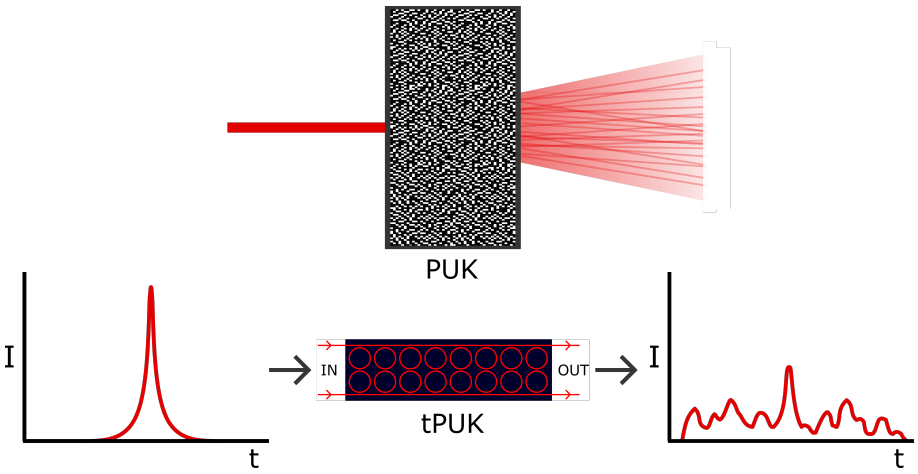

Figure 2.1: *Top* : An illustration that shows how a scattering medium can act as a PUK. Coherent light incident on the PUK is scattered into a speckle pattern. The pattern is uniquely associated with the specific PUK. *Bottom* : An illustration of how a ring resonator system can act as a tPUK by scrambling an incoming optical pulse in time. Figure inspired by [10].

A time-domain physical unclonable key (tPUK) is in essence very similar to a PUK. The difference being that a tPUK's unclonable properties come from the transformation it applies on an optical signal in the time domain as opposed to the spatial domain. As time-domain transformations are generally more easily preserved than spatial transformation during long-distance propagation of a signal, tPUKs are of particular interest in security applications for long-distance networks.

A tPUK's response in the time domain can be concretely described by different optical frequencies having a different and random phase delay when transmitted through the tPUK. This results in a scrambling of the incoming signal in the time domain as illustrated in the bottom section of figure 2.1. Although a scattering medium can also perform such a transformation in the time domain, it is not considered to be a good tPUK. For a scattering medium to possess a complex tPUK-like time-domain transformation it must be relatively thick in the direction of propagation of the signal. Otherwise, it would only be able to introduce relatively short phase delays that can only produce a negligible change in the time structure of an incoming signal. However, a scattering medium of considerable thickness is always characterized by a very low transmission, making it unsuitable for most tPUK purposes [15–18] as well as the particular network security applications that are of interest to us. The transformation a tPUK performs will be made more concrete with a theoretical model presented in the next subsection.

2.1.1 Transmission model of a tPUK

Let us first consider the theoretical model for the input and output field relation of a PUK/tPUK. This will serve as essential background for the theory of (temporal) wavefront shaping discussed later in this chapter.
PUKs are conventionally modeled as one would model scattering media [19, 20]. They can be represented by a square transmission matrix T of size N, where N represents the number of input modes, that relates the input field E^{in} to the output field E^{out}. A single output mode E_m^{out} is determined by the m^{th} row of matrix T. This row can be represented as a sum over the individual row elements t_{mn} multiplied by the n^{th} input mode E_n^{in}. Writing the input field modes in a general form as $E_n^{in} = A_n e^{i\phi_n}$, we have:

$$E_m^{out} = \sum_{n=1}^{N} t_{mn} A_n e^{i\phi_n} \tag{2.1}$$

Now consider a tPUK where, instead of a large number of time-independent spatial input modes, the time-dependent input field consists of a single spatial mode and a set of N frequency modes. The corresponding set of frequencies, Ω, is assumed to be evenly spaced with frequency δ.

$$\Omega = \{\omega_0, \omega_0 + \delta, ..., \omega_0 + (N-1)\delta\} \tag{2.2}$$

Similar to the PUK transmission model we can now relate the n^{th} frequency input mode to the m^{th} spatial output mode using complex matrix elements t_{mn}. It is worth mentioning that the tPUK candidates studied in the lab only posses two spatial outputs. This section is meant to provide a general model that provides a description for a tPUK with an arbitrary number of spatial output modes, M. Writing the time-dependent input field in a general form as $E_n^{in}(\tau) = A_n e^{i[(\omega_0 + n\delta)\tau + \phi_n]}$, the m^{th} spatial output mode is then given

by:

$$E_m^{out}(\tau) = \sum_{n=0}^{N-1} t_{mn} E_n^{in}(\tau) = \sum_{n=0}^{N-1} t_{mn} A_n e^{i[(\omega_0 + n\delta)\tau + \phi_n]} \tag{2.3}$$

In order to more concretely describe the matrix elements t_{mn} another two assumptions are considered that follow from the characteristics of an ideal tPUK. We consider every n^{th} frequency input mode to acquire a random phase factor when propagating through the tPUK. Furthermore we assume the tPUK to distribute the outgoing intensity evenly over all M spatial output modes. With these final assumptions in mind we arrive at the following expression for t_{mn} :

$$t_{mn} = \frac{1}{\sqrt{M}} e^{i\theta_{mn}}, \text{ where } \theta_{mn} \in [0, 2\pi) \text{ with probability function } f_{\Theta_{mn}} = \frac{1}{2\pi} \tag{2.4}$$

The transmission matrix theory detailed here will be utilized further in theory section 2.3 on temporal wavefront shaping.

2.1.2 tPUK ring resonator systems

The integrated tPUKs studied in this thesis consist of systems of coupled ring resonators. This section will discuss the characteristics of ring resonators as well as how systems of ring resonators can lead to tPUK-like transmission characteristics.

A basic ring resonator is made up of a looped optical waveguide and a coupler to access the loop. See figure 2.2 for and example. Only light with a wavelength that fits an integer number of times into the loop's optical path length is able to resonate in the loop [21]. Only these wavelengths will acquire a 2π phase shift on a round-trip through the loop and constructively interfere in the loop. This condition for the resonant wavelengths is expressed in the following equation:

$$\lambda_{res} = \frac{n_{eff} L}{m} \ , \ m = 1, 2, 3, ... \tag{2.5}$$

Where L is the physical length of the loop and n_{eff} the effective refractive index experienced by the light in the waveguide. Light around resonant wavelengths will acquire a significant phase shift when traveling through a ring resonator. The magnitude of this phase shift is determined by the strength of the coupling to the loop and the propagation losses in the loop. The strictness of the resonance condition is also determined by the strength of the coupling to and from the loop. For strong coupling, the resonances of the ring resonator are broader. Light spends less time in the ring and interference in the ring thus has a smaller effect. The spacing of a loop's resonant wavelengths is called the free spectral range (FSR). Assuming no dispersion for n_{eff}, the FSR is given by:

$$FSR = \frac{\lambda^2}{n_{eff} L} \tag{2.6}$$

So a single ring resonator will introduce a phase shift for wavelengths spaced by the FSR. This response is far too simple to be considered tPUK-like. However, multiple ring resonators can be combined into a larger structure in order to create a seemingly random wavelength-dependent phase response. When multiple ring resonators with slightly different FSR's are combined some of the rings individual resonances start to overlap with

each other. As more rings are added the overlap between the resonances becomes increasingly intricate, making the resulting wavelength-dependent phase delay added by the total structure exceptionally random looking.

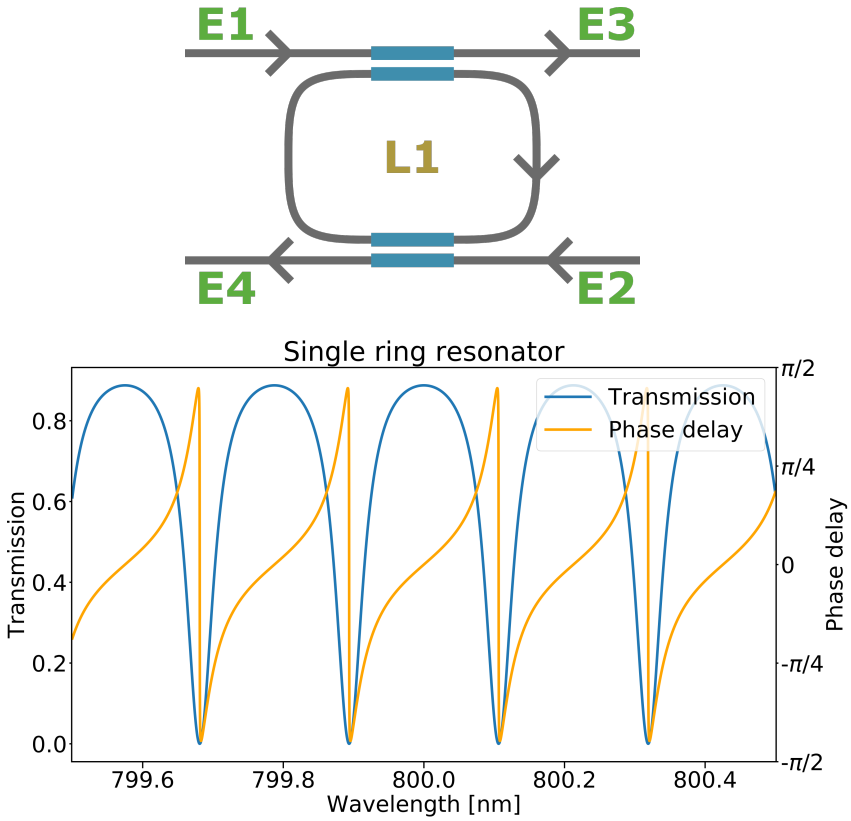

Figure 2.2: *Top* : A sketch of a single ring resonator structure connecting two waveguides. The input and output field are denoted as E1, E2 and E3, E4 in the figure. The blue rectangles represent the coupler to the ring. *Bottom* : An example of the absolute transmission and phase delay from E1 to E3 found for a single ring resonator. Simulated using a model discussed in section 2.2.

2.2 tPUK unit cell model

For our tPUK applications, it is important to design a system with at least two outputs. To realize this, one can equip a ring resonator with two couplers in order to couple to two waveguides, as depicted in figure 2.2. In addition, a second ring resonator is introduced between the two waveguides to ensure light will always travel through the system in the forward direction. See figure 2.3 for a sketch of this design, as well as its transmission characteristics.

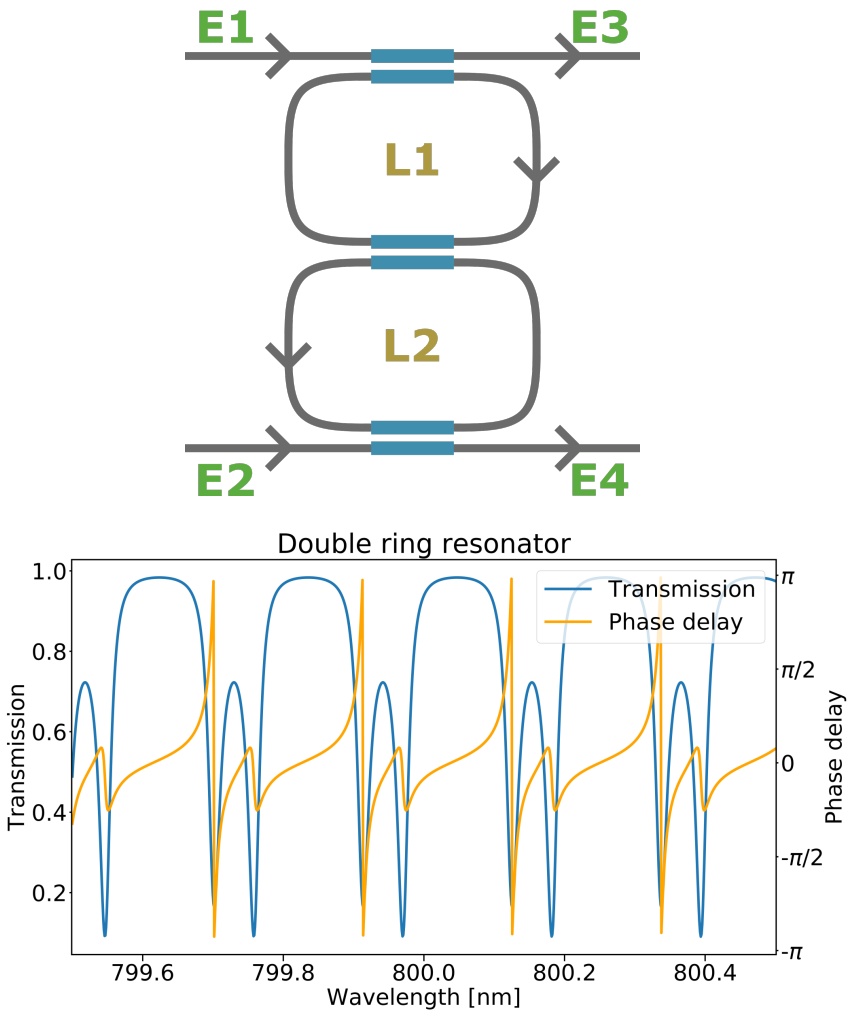

Figure 2.3: *Top* : A sketch of a double ring resonator structure connecting two waveguides. The input and output field are denoted respectively as E1, E2 and E3, E4 in the figure. The blue rectangles represent the couplers to the rings. *Bottom* : An example of the absolute transmission and phase delay from E1 to E3 found for a double ring resonator.

In order to verify that the design presented in figure 2.3 is suited as a unit cell for a larger system, a mathematical model of such a system is needed. To easily combine multiple unit cells into a larger system a transmission matrix model is used. In the model propagation through a ring resonator is taken into account as well as propagation through the couplers. Other components of the structure such as the two straight waveguides are neglected.

2.2.1 Model parameters

In order to derive a model for the total unit cell transmission we first have to mathematically describe the individual components present in the unit cell. We model the couplers as lossless ideal directional couplers featuring a coupling ratio K. For light passing through the coupler we can describe the transformation the coupler applies on the electric field as a multiplication with a constant factor: $C = \sqrt{1 - K_i}$. With K_i the intensity coupling ratio of the ith coupler. Light crossing over in a coupler will experience a different factor. Namely: $-iS = -i\sqrt{K_i}$. It being a complex number follows from the $\pi/2$ phase shift that crossing light undergoes due to energy conservation. Now left is the transmission of light

for a ring resonator round trip. For this the factor $\xi_i = x_i z_i^{-1}$ is used. Where $x_i = e^{-\alpha L/2}$ is the round trip loss coefficient of the ith ring with loss parameter α and ring length L. ${z_i}^{-1} = e^{-i\beta L}$ is the Z transform parameter where $\beta = kn_{eff}$ is the propagation constant, with $k = 2\pi/\lambda$ being the wave number in vacuum. Note that, following from the previous expressions, only the ξ_i terms are able to provide a wavelength-dependent contribution to the final transmission matrix. Having established the mathematical representation of the couplers and the rings a transmission matrix of a unit cell can be determined using Mason's rule [22].

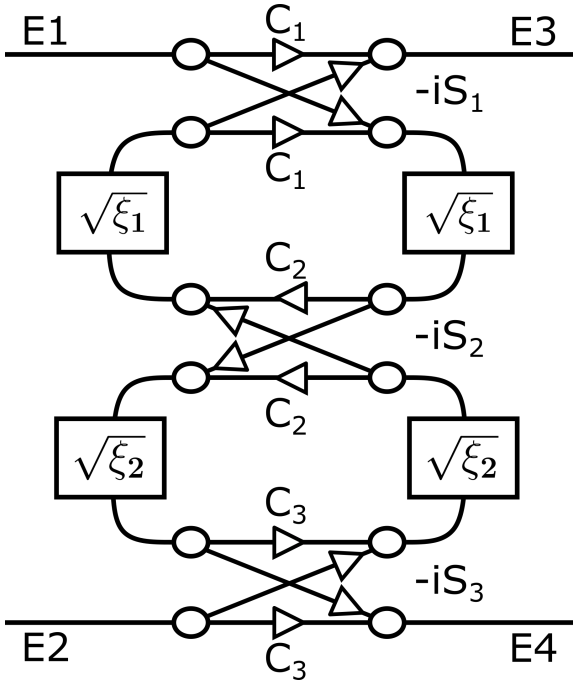

Figure 2.4: The signal flow graph representation of a double ring resonator structure connecting two waveguides. The input and output fields are denoted respectively as E1, E2, and E3, E4 in the figure. Notice the square roots of the ring transmission coefficients are given to signal the travel of a half ring length. The coupling coefficients C_i and S_i are provided for every directional coupler.

2.2.2 Mason's rule

Mason's rule can be used to determine the transfer function for the electric field from one node to another in a signal flow graph (SFG) such as figure 2.4. In the figure, the nodes are represented by the small circles along the waveguide paths. Generally one has to solve a linear system of equations to find the transfer function between two nodes. Mason's rule constitutes to using a determinantal expansion approach to solve such a system of equations. Before using Mason's rule one first has to determine all possible forward paths between the two nodes of interest. A forward path is a sequence of connected nodes along the ring direction that light can use to travel from the starting node to the final node. Such a forward path will have a total gain associated with it determined by the components, such as couplers and ring lengths, encountered on that specific path. In addition to forward paths one has to also consider all loops possible in the total SFG. A loop is in essence a forward path that begins and ends at the same node. With these definitions in mind, we can now use Mason's rule to find the transfer function, H, between two nodes in a SFG.

Concretely Mason's rule states:

$$H = \frac{1}{\Delta} \sum_{i=1}^{N} T_i \Delta_i \tag{2.7}$$

Where Δ is the determinant of the total SFG, T_i is the i^{th} forward path gain between the two nodes and Δ_i is the total determinant excluding loops that touch the path T_i. Equation 2.7 represents a sum over the products of all possible forward path gains and their respective determinants divided by the total determinant of the SFG. The SFG determinant, Δ, is given by:

$$\Delta = 1 - \sum_{i} L_i + \sum_{i,j} L_i L_j - \sum_{i,j,k} L_i L_j L_k \tag{2.8}$$

Where L_i is the total gain of the i^{th} loop. The determinant only includes products of non-touching loops.

2.2.3 Transmission matrix

A transmission matrix representation of a unit cell is useful to relate the input fields to the output fields for that particular unit cell. Mathematically this relation is written as:

$$\begin{pmatrix} E_3 \\ E_4 \end{pmatrix} = M(\lambda) \begin{pmatrix} E_1 \\ E_2 \end{pmatrix} = \begin{pmatrix} t_{00}(\lambda) & t_{01}(\lambda) \\ t_{10}(\lambda) & t_{11}(\lambda) \end{pmatrix} \begin{pmatrix} E_1 \\ E_2 \end{pmatrix} \tag{2.9}$$

In order to determine the transmission matrix elements using Mason's rule we first need to determine all possible loop paths of the unit cell SFG as well as all possible forward paths for each matrix element.

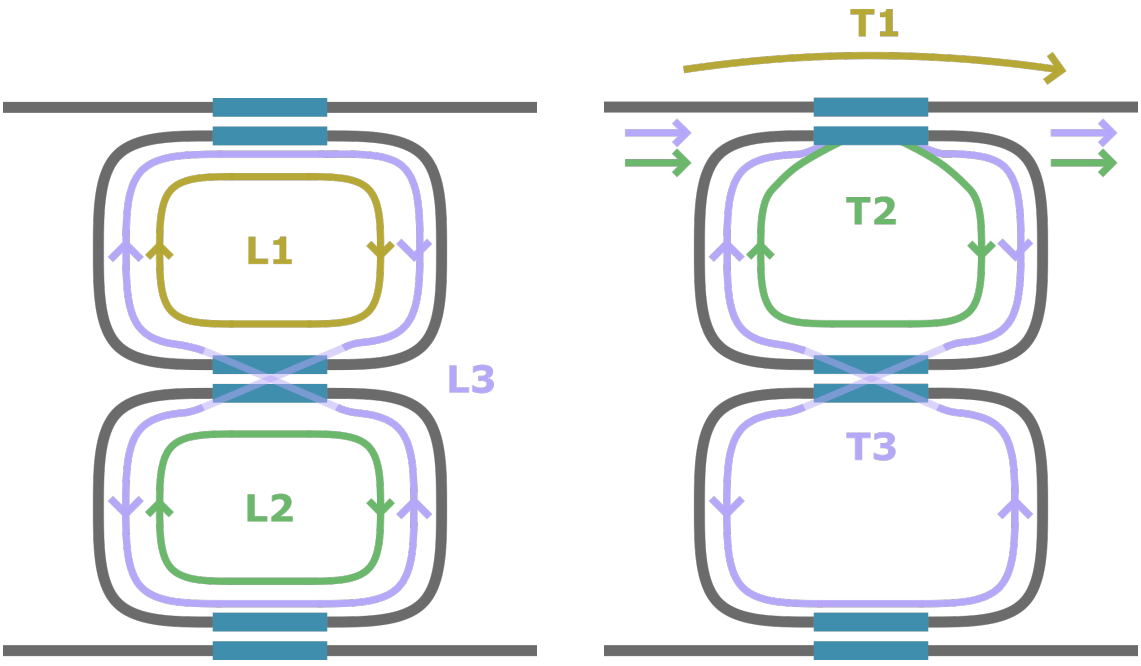

Figure 2.5: *Left*: A sketch displaying all possible loops in the unit cell. *Right*: A sketch displaying the forward paths possible from E1 to E3.

For the tPUK unit cell design there are three possible loops and their respective transmission gains as illustrated in figure 2.5:

$$\begin{array}{lll} \text{Loop 1:} & L1 = C_1C_2\xi_1, & \text{(First ring)} \\ \text{Loop 2:} & L2 = C_2C_3\xi_2, & \text{(Second ring)} \\ \text{Loop 3:} & L3 = -C_1C_3S_2^2\xi_1\xi_2, & \text{(Both rings combined)} \end{array}$$

Where L1 and L2 are non-touching loops.

With these loop gains we can calculate the total determinant of the SFG:

$$\Delta = 1 - (L_1 + L_2 + L_3) + L_1L_2 \tag{2.10}$$

Next the forward paths for every transmission matrix element need to be determined. Starting with the element $t_{00}(\lambda) = E_3/E_1$.

There are three possible forward paths from E_1 to E_3, as illustrated in figure 2.5. Mathematically, these paths are represented as:

$$\begin{array}{llll} \text{Path 1:} & T_1 = C_1, & \Delta_1 = \Delta, & \text{(No ring traveled)} \\ \text{Path 2:} & T_2 = -S_1^2C_2\xi_1, & \Delta_2 = 1 - L2, & \text{(First ring traveled once)} \\ \text{Path 3:} & T_3 = S_1^2S_2^2C_3\xi_1\xi_2, & \Delta_3 = 1, & \text{(Both rings traveled once)} \end{array}$$

Filling in the possible path gains and loop gains into equation 2.7 and using the relation $S_i^2 + C_i^2 = 1$ (lossles coupler), the following expression for $t_{00}(\lambda)$ is found:

$$t_{00}(\lambda) = \frac{X_1}{\Delta} = \frac{C_1 - C_2\xi_1 - C_1C_2C_3\xi_2 + C_3\xi_1\xi_2}{1 - C_1C_2\xi_1 - C_2C_3\xi_2 + C_1C_3\xi_1\xi_2} \tag{2.11}$$

Next we determine the transmission matrix element $t_{01}(\lambda) = E_3/E_2$.
There is only one possible path through the unit cell for light at node E_2 to contribute to E_3:

$$\text{Path 1:} \quad T_1 = iS_1S_2S_3\sqrt{\xi_1\xi_2}, \quad \Delta_1 = 1, \quad \text{(Both rings partially traveled)}$$

Again we use Mason's rule to determine the final expression for the matrix element:

$$t_{01}(\lambda) = \frac{iS_1S_2S_3\sqrt{\xi_1\xi_2}}{1 - C_1C_2\xi_1 - C_2C_3\xi_2 + C_1C_3\xi_1\xi_2} \tag{2.12}$$

The final two matrix elements t_{10} and t_{11} can be derived in similar manner as t_{00} and t_{01}, due to the similar nature of the unit cell design. Taking care to use the correct lengths and coupling coefficients the final expressions for t_{10} and t_{11} are derived as follows:

$$t_{10}(\lambda) = \frac{iS_1S_2S_3\sqrt{\xi_1\xi_2}}{1 - C_1C_2\xi_1 - C_2C_3\xi_2 + C_1C_3\xi_1\xi_2} \tag{2.13}$$

$$t_{11}(\lambda) = \frac{X_2}{\Delta} = \frac{C_3 - C_2\xi_2 - C_1C_2C_3\xi_1 + C_1\xi_1\xi_2}{1 - C_1C_2\xi_1 - C_2C_3\xi_2 + C_1C_3\xi_1\xi_2} \tag{2.14}$$

By combining these expressions for the individual transmission matrix elements the final expression for the whole transmission matrix of a unit cell can be written as:

$$M(\lambda) = \frac{1}{\Delta}\begin{pmatrix} X_1 & iS_1S_2S_3\sqrt{\xi_1\xi_2} \\ iS_1S_2S_3\sqrt{\xi_1\xi_2} & X_2 \end{pmatrix} \tag{2.15}$$

The transmission matrix for a system of multiple unit cells is found by multiplying their individual transmission matrices together. The model derived here is put into practice to compare with experiments in chapter 4.

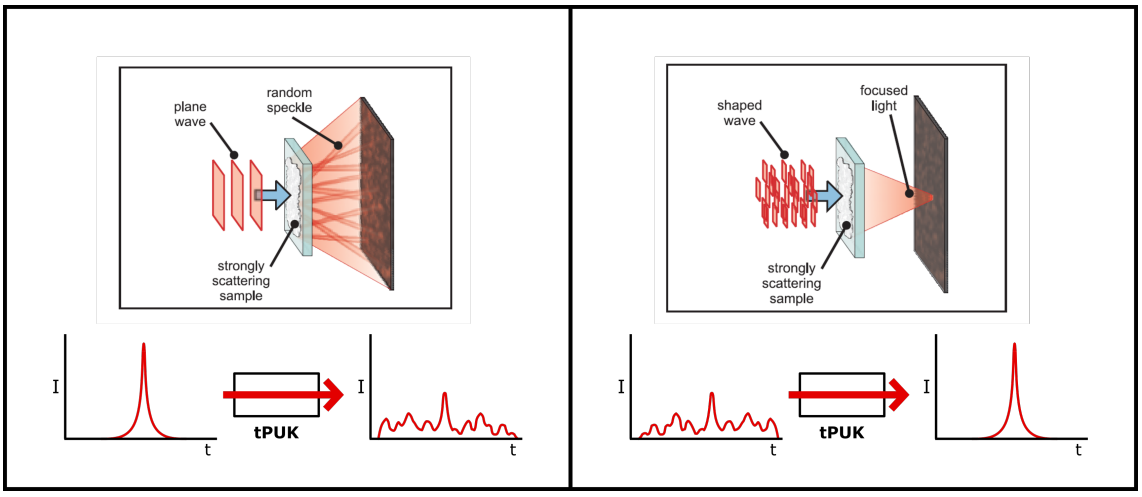

Figure 2.6: *Left* : An illustration showing the similarities between scattering coherent light in the spatial domain performed by a scattering medium and scrambling an optical pulse in the time domain performed by a tPUK. *Right* : Wavefront shaping can produce a focus behind a scattering medium. Similarly temporal wavefront shaping is able to undo the scrambling performed by a tPUK. Figure adapted from [10]

2.3 Wavefront shaping ultra-short pulses

To undo the temporal randomization imposed by the tPUK temporal wavefront shaping is required. This method is very similar to spatial wavefront shaping, a method where one shapes individual segments of an input's wavefront in space. See figure 2.6 for an example of this spatial phase shaping. It should be apparent from equation 2.1 that when the input phase is shaped such that $\phi_n = -\arg(t_{mn})$ all spatial inputs will interfere constructively to maximize the output intensity $|E_m^{out}|^2$.
For a tPUK, there is no use in shaping in the spatial domain, as there is only one spatial input mode. Instead one can employ temporal wavefront shaping and individually shape the phases of the large number of frequency input modes. This is illustrated in the bottom section of figure 2.6. By setting $\phi_n = -\arg(t_{mn})$, all input modes now constructively interfere in time and maximize $|E_m^{out}(\tau = 0)|^2$, where τ is the time parameter. It is interesting to note that for an unshaped input ($\phi_n = 0$), the transmission matrix elements t_{mn} can be directly retrieved from the Fourier coefficients of the tPUK's output signal. This means that setting the ideal input phase $\phi_n = -\arg(t_{mn})$ is essentially the same as taking the tPUK's output signal and conjugating its Fourier coefficients. The ideal input signal is thus given by the temporal structure of the unshaped output but then reversed in time. This fact seems intuitive as one can imagine that inputting the reverse of a scrambled signal back into the scrambler will return an unscrambled output.

A device typically used to perform temporal wavefront shaping is called a pulse shaper [23]. Such a device can modulate the phases of frequency modes with a certain spectral resolution. In addition to enabling temporal wavefront shaping a pulse shaper is interestingly enough also the device that poses one of the largest threats to tPUK security schemes, as discussed in subsection 2.4.2. The physical details of the pulse shaper used in our experimental setup are be discussed in subsection 3.1.4.

2.3.1 Enhancement for temporal wavefront shaping

It is useful to introduce a figure of merit to quantify how well one is able to maximize the output intensity using either spatial or temporal wavefront shaping. The figure of merit typically used for this is called enhancement. For spatial wavefront shaping enhancement η is defined as the ratio between the intensity measured in the shaping region after optimization, $\langle I_N \rangle$, and the measured intensity for the same optimized input but now averaged over different samples, $\langle I_0 \rangle$ [20]. So one can write:

$$\eta = \frac{\langle I_N \rangle}{\langle I_0 \rangle} \tag{2.16}$$

As an example imagine the case where one uses wavefront shaping to create a focus behind a scattering medium. To determine the enhancement in this case, one first measures the intensity in the focus, $\langle I_N \rangle$. Subsequently, the scattering sample is shifted to a different position, effectively providing a different sample, and the intensity in the original focus position is measured again. This step is repeated multiple times so one can determine an ensemble-averaged intensity $\langle I_0 \rangle$. One can then determine the enhancement from the ratio between $\langle I_N \rangle$ and $\langle I_0 \rangle$.

For spatial wavefront shaping the enhancement scales linearly with the number of controlled spatial input modes, N, assuming that the scattering medium's complex transmission matrix elements t_{mn} are randomly distributed in accordance with circular Gaussian distribution. The linear scaling is described by the following expression [20]:

$$\eta = \frac{\pi}{4}(N-1) + 1 \tag{2.17}$$

For our temporal wavefront shaping purposes, it is useful to know what level of enhancement to expect. Using equation 2.4 one can find ensemble-averaged expected values for the intensities $\langle I_N(t) \rangle$ and $\langle I_0(t) \rangle$ as derived in [10].

$$\begin{aligned} \langle I_0(t) \rangle &= \frac{N}{M} \\ \langle I_N(t) \rangle &= \frac{1}{M} \frac{\sin^2(N\delta t/2)}{\sin^2(\delta t/2)} \end{aligned} \tag{2.18}$$

Where N are the number of controlled input frequency modes, M the number of spatial output modes, and δ the frequency spacing of the input modes.
From equation 2.18 it becomes clear that the maximum enhancement in time is N as $\langle I_N(t \to 0) \rangle = N^2/M$. However, measuring this enhancement is not as straightforward as it seems. Consider that the temporal features of the output field have a duration of the order $\Delta t \sim 1/N\delta$. For a system using optical pulses the bandwidth $N\delta$ can easily be in the order of a few THz, meaning that the duration of the temporal features of the output field are somewhere in the femtosecond range. Using a regular linear photo detector will thus always result in a time-averaged measurement of the intensity. This can be represented by integrating the intensities $\langle I_N(t) \rangle$ and $\langle I_0(t) \rangle$ over a single optical period, $2\pi/\delta$:

$$\begin{aligned} S_0^1 &= \int_{-\pi/\delta}^{\pi/\delta} \langle I_0(t) \rangle \, dt \; = \frac{2\pi}{\delta} \frac{N}{M} \\ S_N^1 &= \int_{-\pi/\delta}^{\pi/\delta} \langle I_N(t) \rangle \, dt \; = \frac{2\pi}{\delta} \frac{N}{M} \end{aligned} \tag{2.19}$$

Equation 2.19 makes it clear that a time-averaged linear detector is incapable of measuring any enhancement due to temporal wavefront shaping. A different measurement approach has to be considered for any feedback-based temporal wavefront shaping method to be successful.

Linear detectors can still be used for interferometric measurements that reconstruct the temporal features of the output field. Unfortunately these interferometric measurements are rather slow and thus not suitable for feedback based temporal wavefront shaping, where more than a thousand shaping iterations are typically needed before finding an ideal input pulse structure. Instead one can make use of non-linear detectors. By operating in their two-photon absorption range these detectors are capable of measuring a signal proportional to $I^2(t)$. The time-averaged non-linear signal measured then becomes:

$$\begin{aligned} S_0^2 &= \int_{-\pi/\delta}^{\pi/\delta} \langle I_0(t) \rangle^2 \, dt \; = \frac{2\pi}{\delta} \frac{N^2}{M^2} \\ S_N^2 &= \int_{-\pi/\delta}^{\pi/\delta} \langle I_N(t) \rangle^2 \, dt \; = \frac{2\pi}{\delta} \frac{2N^3 + N}{3M^2} \end{aligned} \tag{2.20}$$

The non-linear enhancement then becomes:

$$\eta_{NL} = \frac{S_N^2}{S_0^2} = \frac{2}{3}\left(N + \frac{1}{2N}\right) \tag{2.21}$$

Thus a linear relation is found for the non-linear enhancement. The most important conclusion of this section is that we need to use a non-linear detector in any feedback-based temporal wavefront shaping that we set up. Additionally, it is worth mentioning that the figure of merit when shaping the tPUK input is actually not the general non-linear enhancement derived here. We are more concerned with creating the largest possible non-linear signal ratio for two outputs of the same ring resonator system. In the next section of this theory chapter, it will become clear why specifically this ratio must be maximized when shaping the input of the tPUKs.

2.4 Proposed security applications featuring tPUK's

This section aims to provide some examples of promising tPUK security applications. A major application, tPEAC, is concerned with providing secure communication without the need for an authenticated communication channel or the exchange of secret information. In addition to this tPUKs can also be applied to provide an authenticated communication channel, which will be discussed in a later subsection.

2.4.1 Secure asymmetric communication

A major application possibility for tPUKs would be their use in methods that provide means of secure communication. Time-domain PUK-enabled asymmetric communication (tPEAC) is a promising method studied earlier in the AQO group. In this method, a sender, Alice, sends information to a receiving party, Bob, who is in the possession of a tPUK. The sending of this information is deemed secure if Alice can be certain that the information they send can only be received by Bob and not by some third party, Eve, trying to eavesdrop. The tPEAC scheme provides this security by making use of the temporal scrambling properties of Bob's tPUK in combination with Alice applying time-domain wavefront shaping to send their information. By design, Bob's tPUK will possess

two spatial outputs. Light exiting at one output will have been temporally scrambled in a way unique to that output. By using temporal wavefront shaping, Alice can now choose which output's scrambling to undo. This allows her to create a pulse in an output of her choice, effectively sending either a '1' or a '0'. A sketch illustrating the tPEAC method is given in figure 2.7.

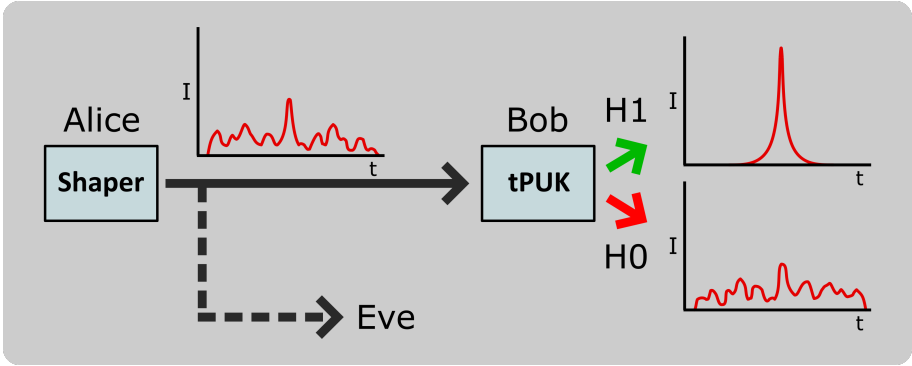

Figure 2.7: A schematic overview of the tPEAC communication method. Alice uses a pulse shaper to securely send a message to Bob. If Alice uses a superposition of wavefronts belonging to the H_1 set Bob's tPUK will produce an optical pulse in the corresponding output. The same holds for H_0. Figure adapted from [10].

A natural extension to secure communication is providing authentication. In the tPEAC method, Bob's authenticity is inherently proven as only they are in possession of the correct tPUK. For two-way authentication, the scheme can be expanded with the condition that Alice is in the possession of their own tPUK as well. If Bob then needs to verify the message they received was indeed from Alice they only need to ask Alice for confirmation in wavefronts encoded specifically for Alice's tPUK [24]. An authentication protocol such as this could be very useful in situations where the authority of communicating parties is essential and needs to be proven.

2.4.2 Security

The tPEAC scheme described above provides a means of secure communication without relying on secret information shared between Alice and Bob. The scheme can only function if two essential conditions are met:

Key imitation:
A third party, Eve, should not be able to replicate or emulate Bob's tPUK. Due to the unclonable properties of a tPUK Eve will not be able to replicate Bob's tPUK, they can, however, try to mimic the temporal scrambling that Bob's tPUK performs using a pulse shaper of their own, as illustrated in figure 2.8 a). The best defense against this attack strategy is ensuring that the spectral resolution of Bob's tPUK is greater than that of Alice's pulse shaper. This condition ensures that Bob's tPUK will possess a larger number of independent frequency channels, N^*, than the number of controllable frequency modes Alice's pulse shaper possesses, N. As a consequence, there is not one single unique wavefront that maps to one of the tPUK outputs. Instead, there will exist a set of wavefronts, H_0, that maps to output '0' and a set, H_1, that maps to output '1'. Alice is then able to send any random superposition of wavefronts in H_0 or H_1 and Eve will not be able to mimic the tPUK as the superposition that Alice sends is unknown to

them [11].

Wavefront estimation:
In the tPEAC protocol, Alice will be sending information encoded in superpositions of wavefronts belonging either to the H_0 or H_1 sets. It is thought to be Eve's optimal attack method to try and read out or estimate the wavefronts Alice is sending [11]. Alice can protect against wavefront estimation attacks by sending wavefronts using average photon numbers, ($\langle n \rangle$), much smaller than the number of controllable modes, N. Then Eve will have to employ quantum state estimation methods to determine which set the wavefronts Alice sends belong to. This is illustrated in figure 2.8 b). The most powerful state estimation method Eve can employ is based on universal cloning [11, 25] and yields a correct estimation of the wavefront with a probability:

$$P_{estimate} = \frac{1}{q} + \frac{\langle n \rangle}{N} \frac{N-1}{N+\langle n \rangle} \tag{2.22}$$

With q being the number of tPUK outputs. It is evident from equation 2.22 that for a tPUK featuring two outputs, the correct guess chance $P_{estimate}$ goes towards 1/2 if Alice ensures the condition $N \gg \langle n \rangle$ is met. Thus protection against wavefront estimation is provided, as a 50/50 chance of correctly estimating the state is no better than a random guess. Pulse shapers commonly allow for a number of controllable modes, N, in the order 1000. Thus Alice will need to send wavefront with $\langle n \rangle$ ranging in the tens of photons. Such low photon numbers will require Bob to utilize sophisticated non-linear detection methods or time-gated detection in order for them to properly measure the output signals of their tPUK. Increasing the number of spatial outputs will lower the strictness of the low mean photon number condition. For example, for four spatial outputs $P_{estimate}$ is approximately 1/2 if $\langle n \rangle \approx 300$.

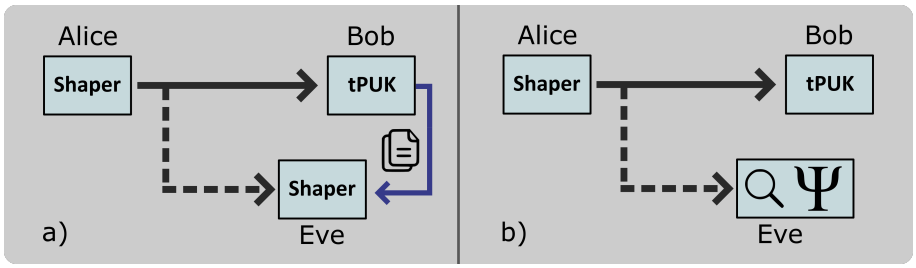

Figure 2.8: *a)* : A schematic overview of a key imitation attack where Eve copies the properties of Bob's tPUK. *b)* : A sketch of a wavefront estimation attack where Eve uses quantum state estimation to determine what wavefront Alice has send.

3. Experimental methods

For the purposes of characterization and demonstration of the fabricated tPUK chips, an experimental setup is required that consists of two main parts. The first is a Michelson interferometer used for the characterization of the tPUK chips. The second part of the setup consists of a pulse shaper to shape the chip input in the time domain and a non-linear detection section that provides feedback for the temporal wavefront shaping algorithm.

3.1 Setup

Figure 3.1 shows a schematic overview of the lab setup. It consists of a pulsed laser source, a chip sample, a Michelson interferometer, a pulse shaper and a non-linear detection section.

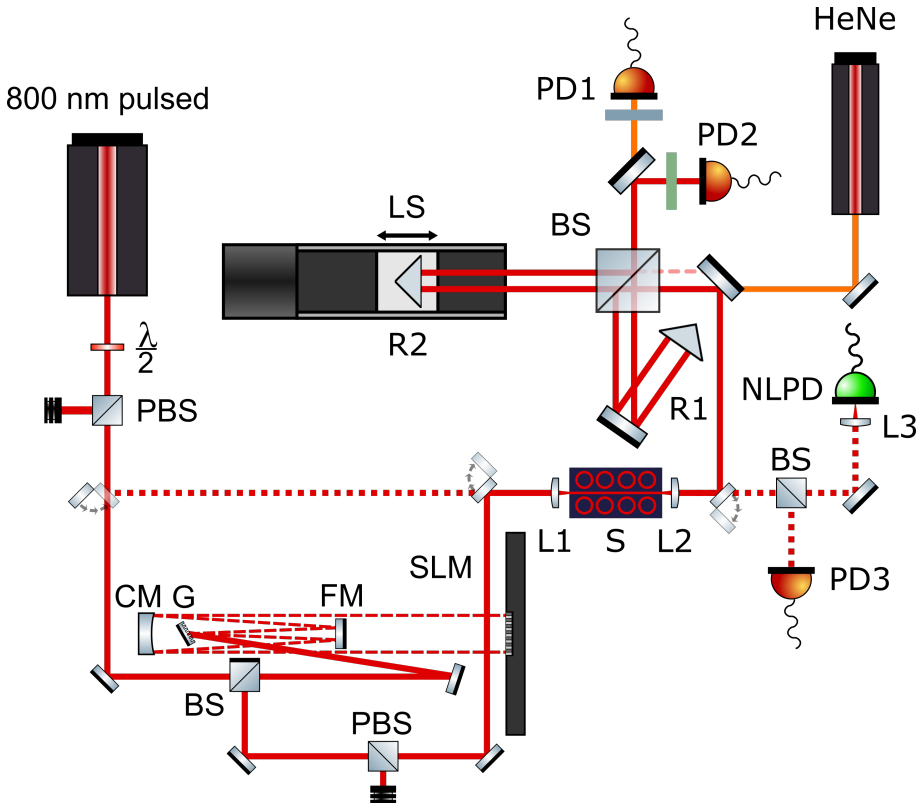

Figure 3.1: A schematic overview of the lab setup. Labels used: $\lambda/2$: half wave plate, (P)BS: (polarizing) beamsplitter, CM: cylindrical mirror, FM: folding mirror, G: grating, L: lens, LS: linear stage, (NL)PD: (non-linear) photodiode, R: retro-reflector, S: integrated tPUK sample, SLM: spatial light modulator. Auxiliary instruments or components have not been drawn.

3.1.1 Laser source

The laser source is a femtosecond pulsed Ti:Sa laser (Spectra Physics Tsunami 3960). The laser is pumped at 7.0 W with a 532 nm continuous wave (CW) pump laser (Spectra Physics Millenia Xs). The pulsed laser has a maximum output power of approximately 1.4 W. It is tuned to produce ultra-short femtosecond pulses with a center wavelength of 800 nm and a bandwidth of 13 nm, with a repetition rate of 80 MHz. To provide attenuation and ensure horizontal polarization a half-wave plate and polarizing beamsplitter are situated at the output of the laser source. Also present but not drawn in the setup figure, is a fiber spectrometer used to measure the laser output (Avantes, ~ 0.5 nm/pixel). The pulses produced by the laser source have a sech^2 shape [26], with their spectrum described as:

$$I(\nu) = A\ \text{sech}^2\left(\frac{1.763\nu}{\Delta\nu}\right) \tag{3.1}$$

With A being the spectral amplitude, ν the optical frequency and $\Delta\nu$ the full width at half maximum (FWHM) [27, 28]. See figure 3.2 for a spectrum of the laser source. A bandwidth of 13 nm is chosen as it is roughly the maximum achievable bandwidth before the laser source becomes unstable. A large bandwidth is desirable as it increases the maximum number of controllable wavelengths for the pulse shaper. Additionally, a large bandwidth produces pulses with a higher peak intensity that is more easily detected using a non-linear detector.

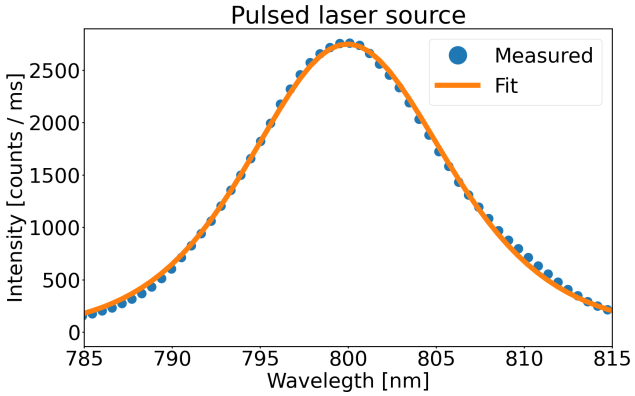

Figure 3.2: The spectrum of the pulsed laser source, as measured by the fiber spectrometer. The pulse has a bandwidth of 13 nm. The expression for the sech^2 fit is given in equation 3.1.

3.1.2 Photonic chip sample

In cooperation with LioniX, six integrated tPUK chips were fabricated. The chips are based on a silicon-nitride waveguide platform TriPleX [29]. The photonic chips measure 1.6 cm in length and 0.8 cm in width. Every chip is fabricated with 6 ring resonator systems. Every system has two inputs and two outputs, resulting in a total of 12 chip inputs and outputs. Further details of the chip design are given in section 4.1. The chips are placed on top of a heating element using thermally conductive tape to stabilize the temperature of the chips, as can be seen in the left section of figure 3.3. The heater keeps the chips at a stable temperature of 35.0 °C. Coupling light into and out of the chip is performed using the lenses marked L1 and L2 in setup figure 3.1. These lenses are aspheric

lenses (Thorlabs A220 TM) that roughly match the 4 mm $1/e^2$ beam diameter of the laser source. These lenses are situated on electronically controlled 3D piezo translation stages (Smaract mcs-1) that can move with nanometer precision. Light can be coupled into a chip input of choice by setting the position of the input stage. Similarly, an output of choice can be selected by setting the position of the output translation stage. The chip input and output facets are spaced by 125 μm, so precise control of the input and output coupling lenses is essential. A CCD camera (Guppy PRO F125B) is situated above the photonic chip sample to provides a visual aid when manually aligning the input and output coupling lenses. As can be seen in the camera image shown in the right section of figure 3.3, the camera view clearly displays what system light is coupled into.

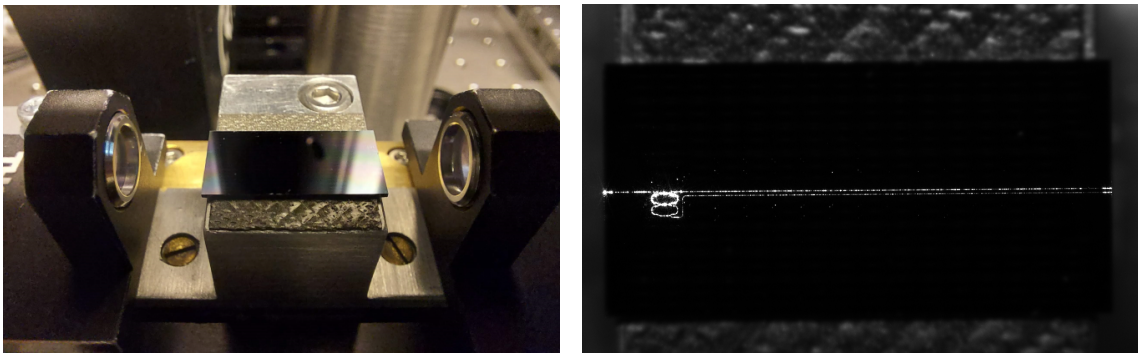

Figure 3.3: *Left*: A picture of the chip samples in the lab. Also visible are the two lenses used for input and output coupling. *Right*: A camera image from the camera situated above the chip. The single unit cell system is active here, as can be seen from the scattered light captured by the camera.

3.1.3 Michelson interferometer

To characterize the photonic tPUK chips it is necessary to measure their transmission response in the frequency domain. A Michelson interferometer is used in combination with Fourier interferometry to determine the output power spectra of the sample chips. As illustrated in setup figure 3.1, the Michelson interferometer consists of two interferometer arms. While one arm has a fixed length, the length of the other arm can be adjusted by moving a linear translation stage (Newport M-ILS150PP). By adjusting the arm length we are able to perform an auto-correlation on light coming from the output of the chip sample. Assuming a 50:50 beamsplitter, the measured interferometric auto-correlation signal is given by:

$$A(\tau) = \int_{-\infty}^{\infty} \left| E_{out}(t) + E_{out}(t-\tau) \right|^2 dt \tag{3.2}$$

Where $E_{out}(t)$ is the output electric field and τ the relative delay in time introduced by changing the length of the adjustable interferometer arm. Having measured the auto-correlation of the signal, the power spectrum of the signal can be retrieved by applying the Fourier transform on the auto-correlation, $S(\omega) = \mathcal{F}\{A(\tau)\}$. This relation is called the Wiener–Khinchin theorem. Before Fourier transforming the auto-correlation, first its mean value is subtracted to remove the DC term in the power spectrum.

To allow for accurate measurement of the auto-correlation signal, one has to ensure that the time delay steps between measurements of the signal are as equidistant as possible

when scanning the adjustable interferometer arm. The velocity with which the linear translation stage moves is however not stable enough to ensure this equidistant sampling condition. A frequency stabilized Helium-Neon (HeNe 632.8 nm) CW laser source is added as a reference to ensure equidistant sampling. Measurements of the auto-correlation signal are triggered using the zero-crossing points of the interference pattern of the HeNe laser source. The HeNe operates at a wavelength of 632.8 nm. Thus it is ensured that a sample of the signal is taken every 316.4 nm of optical path length difference. The output signals of the Michelson interferometer are separated with a Bragg mirror and measured using two linear photodiodes (Thorlabs PDA 55). One for the 800 nm chip output, PD2, and one for the 632.8 nm HeNe reference, PD1. Two band-pass filters ensure that these detectors exclusively measure the intended signals.

The spectral resolution with which one can measure the output spectrum is given by the maximum optical path length difference (ΔOPL) that can be introduced. The linear stage that is used is physically able to introduce a maximum ΔOPL of 300 mm. However, to prevent any edge effects the maximum scan range is limited to 250 mm. With the sampling distance (316.4 nm) and maximum (ΔOPL) (250 mm) known, the spectral resolution can be calculated as follows:

$$\lambda_{res} = \lambda_{sc} - \frac{C}{\nu_{sc} + \nu_{res}}, \quad \nu_{res} = \frac{\nu_{ref}}{2\,N_s}, \quad N_s = \frac{2\,\Delta OPL_{max}}{\lambda_{ref}} \tag{3.3}$$

Here λ_{sc} and ν_{sc} are the center wavelength and frequency of the chip output, ν_{res} is the spectral frequency resolution, λ_{ref} and ν_{ref} are the wavelength and frequency of the HeNe reference and N_s is the number of samples taken. Mind the factor two in the frequency resolution. This is because a double-sided frequency spectrum is obtained from the Fourier transform of the auto-correlation. Filling in the known quantities of the linear stage, reference, and pulsed laser source, the following spectral resolution is obtained: λ_{res} = 2.6 pm.

3.1.4 Pulse shaper

A pulse shaper is included in the setup in order to enable time-domain wavefront shaping of the chip input. The pulse shaper present in the lab is set up in a 4f configuration. See the top left of figure 3.4 for an illustration of a 4f pulse shaper. In a 4f pulse shaper, a pulse is first incident on a grating. The pulse is dispersed by the grating and subsequently collimated by a lens with focal length f. At a distance 2f away from the grating, in the Fourier plane, light encounters a phase mask. Because of the dispersion introduced earlier by the grating, optical frequency varies linearly with the horizontal coordinate at the location of the phase mask. Having traveled a distance f further past the phase mask light is collected by a lens with focal length f and focused onto a grating with the same properties as the first grating encountered. This final grating combines the light back into an output pulse. The total distance from the initial grating to the final grating is 4f, hence the name of this configuration. The distance f between all components of the pulse shaper ensures that the device is symmetrical in the Fourier plane so that each optical frequency travels the same optical path through the pulse shaper. Because of this, no dispersion is introduced besides that which the phase mask introduces.

In order to make the pulse shaper more practical and more compact, the 4f pulse shaper present in the lab is set up in a manner a bit different from the one displayed in the top left of figure 3.4. A mirror is placed in the Fourier plane, closely behind the phase mask. Additionally, instead of lenses, a cylindrical mirror is used. To compact the setup further

a folding mirror is placed between the grating and the cylindrical mirror. This design is similar to the design shown in the bottom left of figure 3.4. To separate the input and output signal of the shaper a beamsplitter is used. This introduces an attenuation of factor 4 between the in-going and outgoing pulse shaper intensity.

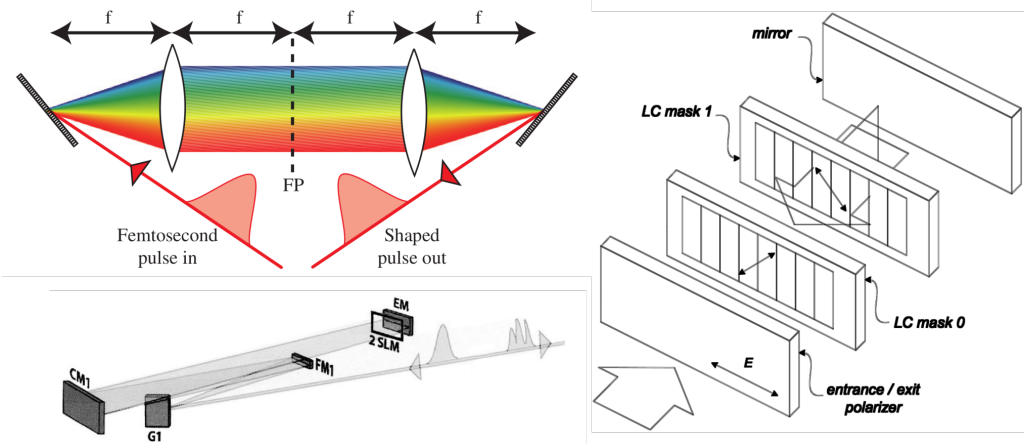

Figure 3.4: *Top left*: A sketch of a 4f pulse shaper. The mask is placed in the Fourier plane, labeled FP. Reproduced from [23]. *Bottom left*: Schematic overview of a symmetric and folded 4f pulse shaper, similar to the setup present in our lab. Labels: CM1: cylindrical mirror, FM1: folding mirror, G1: grating, EM: end mirror, 2SLM: two spatial light modulators (SLM) in a stacked configuration. Adapted from [30]. *Right*: Diagram showing how the SLM in the Fourier plane is made up of two orthogonally polarized liquid crystal masks, with an end mirror closely behind. Amplitude modulation is made possible by adding an additional PBS in the input and output of the pulse shaper. Adapted from [31].

The spectral resolution of the pulse shaper depends on properties such as the grating period or the focal distance of the cylindrical mirror. In the Fourier plane, the dispersion of wavelengths around the center wavelength is given by:

$$\delta\lambda(x) = \frac{d\cos(\theta_d)}{f}x \equiv \alpha x \tag{3.4}$$

Here d is the grating period, θ_d the diffraction angle, f the focal length of the cylindrical mirror and x the horizontal distance from the center wavelength in the Fourier plane [23]. Diffraction angle θ_d, in its turn, is given by the grating equation:

$$\theta_d = \arcsin\left(\frac{\lambda_0}{d} - \sin(\theta_i)\right) \tag{3.5}$$

Where λ_0 is the center wavelength and θ_i the incident angle. A diffraction order of -1 is assumed here [32]. A gold coated grating is used with $d = 1/2000$mm (Spectrogon PC 2000). The focal length of the used cylindrical mirror is 520 mm. These values combined with an angle of incidence of 59° result in a parameter $\alpha \approx 0.64$pm/μm, according to equations 3.4 and 3.5. The mask in the Fourier plane is a spatial light modulator (SLM) that consists of two liquid crystal masks (Cambridge Research & Instrumentation SLM-640-D-VN). The liquid crystal mask are made up of 640 pixels, each with a width of 100 μm and a height of 5 mm. A pixel width of 100 μm thus leads to a spectral resolution of $\alpha \times 100$ μm/pixel ≈ 64 pm/pixel.

As is shown in the right side of figure 3.4, the extraordinary axes of the liquid crystal masks are orthogonally angled, at $\pm 45°$ with respect to the horizontal axis. Using Jones calculation one can find the transfer function for the n^{th} pixel, this is given by:

$$H_n = \exp\left(i\frac{\phi_0(\lambda_n) + \phi_1(\lambda_n}{2}\right)\cos\left(\frac{\phi_0(\lambda_n) - \phi_1(\lambda_n)}{2}\right) \tag{3.6}$$

Here ϕ_0 and ϕ_1 are the phase differences between the extraordinary axis and the ordinary axis of mask 0 and mask 1 respectively. λ_n is the wavelength incident on pixel n [30, 33]. As can be seen in equation 3.6, the final optical phase shift is thus given by the average of the phase difference of the individual masks. The equation also includes a cosine amplitude modulation term. It shows that the preformed amplitude modulation is equal to the cosine of the difference between the masks' phase shifts. This amplitude modulation term can only be included when a polarizing beamsplitter is placed in both the input and output of the pulse shaper. Without those, only phase modulation is possible. Even though the setup in the lab allows for amplitude modulation, only phase modulation is used. Amplitude modulation only provides marginally better shaping results. Furthermore, it adds complexity to the shaping process and may be especially difficult to implement with low signal-to-noise ratios [34].

The phase shifts of the SLM's liquid crystal masks are set by applying a certain voltage to the pixels. This relation between added phase and voltage is highly non-linear. Therefore, calibration of the liquid crystal masks is required. A calibration method based on the amplitude term of equation 3.6 is used. The exact calibration process, explained in [35], is extensively described in previous work by Matthijs Velsink [10]. A wavemeter (MogLabs MWM $\sim$ 1 pm resolution) is used to perform this calibration in a precise and accurate manner. After calibration, the pulse shaper is able to add a phase between 0 and 2π at every pixel. This can be done in steps of $2\pi/1000$. The shaper is able to change the phases added by the liquid crystals at a maximum rate of 5 Hz.

One of the main experimental complications encountered with 4f pulse shapers is spatio-temporal coupling. The spatial beam profile still has a finite width in the Fourier plane for each frequency component. Therefore a phase tilt of the SLM also introduces a spatial phase tilt in the Fourier plane. This tilt in turn causes the output beam for that frequency to shift horizontally. Thus, because of spatio-temporal coupling, altering the temporal wavefront of a beam can also change the beam's spatial wavefront. To reduce spatio-temporal coupling effects, the pulse shaper input must have a large beam diameter. This large beam diameter causes light to be focused strongly in the Fourier plane. After introducing a beam expander before the pulse shaper the input beam has a FWHM, Δx_{in}, of 2.3 mm. The width in the Fourier plane is then [23]:

$$\Delta x_0 = 2\ln(2)\frac{\cos(\theta_i)}{\theta_d}\frac{f\lambda_0}{\pi\Delta x_{in}} \tag{3.7}$$

Using the properties of the pulse shaper, Δx_0 is calculated to be approximately 61 μm. As this is smaller than the pixel width, spatio-temporal coupling effect should be small. The time window available before spatio-temporal effects become too large follows from the Fourier transform of the pulse shaper's frequency resolution and is given by [23]:

$$T = \frac{\Delta x_{in}\lambda_0}{c\, d\cos(\theta_i)} \tag{3.8}$$

Here, c is the speed of light in vacuum. The time T is approximately 24 ps for the parameters of our pulse shaper. This value is comparable to what is typically achieved

in other 4f pulse shapers [23, 30, 33]. This time window, T, is effectively the maximum dispersion the pulse shaper can compensate.

3.1.5 Non-linear detection

A non-linear detection method is included in the setup to provide a feedback signal for the iterative temporal wavefront shaping method used in the lab. As stated earlier in theory section 2.3.1, temporal wavefront shaping can not increase or decrease the total intensity in an output pulse. It can only improve the peak intensity of the pulse. Therefore a non-linear detection method is needed to measure this enhancement. In the lab, light from the chip's output is focused on the non-linear photodiode using identical lenses L2 and L3 (Thorlabs A220 TM). The L2 lens that is used to couple light out of the chip can be used to collimate and displace the output beam. A mirror is placed before lens L3 to also provide control over the beam angle before focusing onto the detector.

The detector that is used is a GaAsP photodiode intended for the detection of visible light (Hamamatsu G1116). The linear absorption of this photodiode ends around 700 nm. Therefore, the absorption around 800 nm is dominated by 2-photon absorption. We can use this 2-photon absorption to measure the squared intensity without a need for phase matching [36–38]. The small output current of the photodiode is amplified by a transimpedance amplifier (Femto DLPCA-200). Due to fluctuations of the chip input coupling efficiency, the total intensity incident on the non-linear photodiode (NLPD) may vary. During temporal wavefront shaping, we would ideally only measure an increase in the non-linear signal due to a higher peak intensity and not due to a larger total pulse intensity. To achieve this the total pulse intensity is measured using a linear photodiode (Thorlabs PDA55), PD3. Before a pulse shaping attempt, the NLPD is characterized for a varying chip output power. Such a relation is shown in figure 3.5.

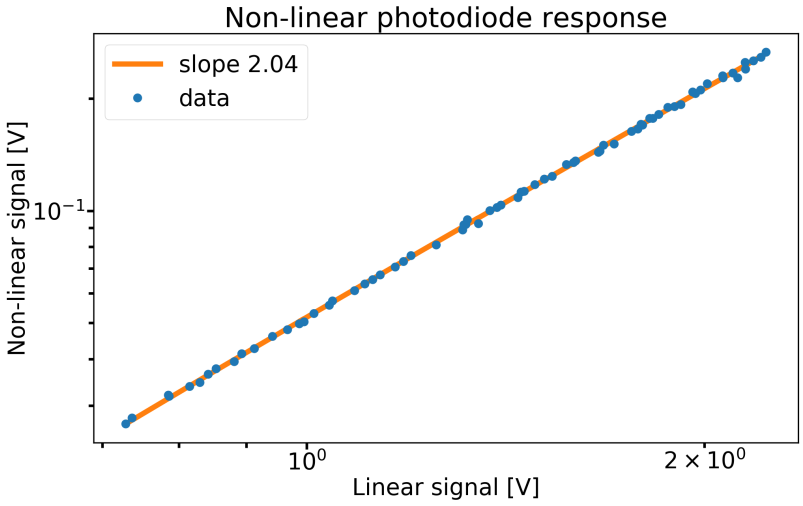

Figure 3.5: A log-log plot of the non-linear photodiode signal as function of the linear photodiode's signal. The largest linear signal corresponds to an output power of approximately 3.5 mW.

The plot shown in figure 3.5 shows that the NLPD signal on a log-log scale is best fitted by a linear fit with slope 2.04. This value very close to 2 indicates that the NLPD's response is dominated by 2-photon absorption. Thus the detector can be used to measure time-domain enhancement and provide a feedback signal to the shaping method.

4. Photonic tPUK chips

The main research effort of this thesis is focused on studying integrated tPUK candidates. This research is a continuation of recent work in the AQO group focused on studying multimode optical fibers, with their complex mode coupling properties [39, 40], as possible tPUK candidates. It was concluded that these multimode fibers show the required tPUK-like properties [10]. However, the response of these fibers is very sensitive to input coupling fluctuations as well as fluctuations of the fiber environment such as bending the fiber [41, 42]. To provide a solution to such problems and move closer towards a tPUK suitable for real-world applications, integrated tPUK designs were put forward [10]. The small dimensions of a photonic chip ($\approx$ 1-2 cm) and the single spatial mode inputs it possesses make it robust against input fluctuations and easier to be shielded against environmental fluctuations. In total, six photonic chips featuring ring resonator systems were designed and fabricated in cooperation with LioniX International. The chips were fabricated using E-beam lithography and are based on low-loss TriPleX silicon-nitride waveguide technology from LioniX [29]. This chapter covers the design of the chips in detail. In addition to this, the experimental and simulation results from the characterization efforts are covered as well.

4.1 Chip design

Of the six chips that were fabricated, three chips were designed with tapers at every chip input and output facet to allow for better coupling to and from the chip. The other three were designed without. The chips in these two groups again differ between themselves with respect to the coupling ratios of the directional couplers featured on these chips. In these groups, the chips use a 40/60, 50/50, and 60/40 intensity coupling ratio respectively. This difference is designed to study the effect the coupling ratio has on developing the resonance overlap in a tPUK system. Every ring resonator system present on a chip features two inputs as well as two outputs. The chips all feature a design that consists of six independent ring resonator systems. The chip design can essentially be split down the middle horizontally into two halves that are designed to be exact copies of each other. As can be seen in figure 4.1, such a half features three different ring resonator systems. The systems consist of double ring resonator unit cells joined together in a serial configuration. From the middle to the edge of the chip the number of ring resonator pairs featured in these systems are 1, 13, and 46 respectively. To promote resonance overlap between the system's unit cells the ring resonators in those unit cells should all be of similar length but differ slightly. To achieve this, the round-trip length of the ring resonators in every unit cell is designed to be 2250 µm. Additionally, a randomized length, L_{rand}, taken from a uniform distribution with a range 0 - 20 µm is added pair-wise to the ring resonator lengths. Finally, the design of the three systems is copied exactly to the other half of the chip. By fabricating these exact copies of systems on the same chip, we are effectively performing a key imitation attack. This way we are able to experimentally study how manufacturing defects contribute to the unclonability of the tPUK systems.

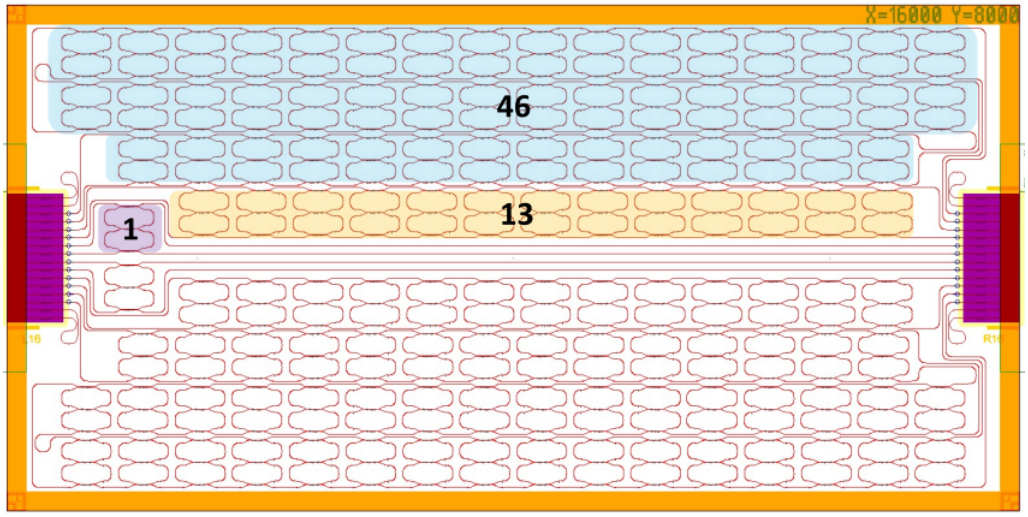

Figure 4.1: A sketch of the photonic chip design as studied in the lab. Six ring resonator systems are positioned on the chip, consisting of 3 unique systems and their counterparts mirrored along the horizontal direction. The total chip dimensions are displayed in micrometers at the top right of the figure. Three independent systems are highlighted in the figure.

4.1.1 System simulations

Simulations of the tPUK systems were essential in determining their final design before fabrication [10]. Now that the chips have been fabricated, simulations can again be used to compare theory with experiment and verify the design parameters of the chips. The model derived in section 2.2 can be used to simulate systems like those fabricated on the photonic chips for an arbitrary number of unit cells. A number of chip design properties are used as input parameters for these simulations:

The number of double-ring resonator unit cells included in the system, $\mathbf{N}$. The intensity coupling ratio of every directional coupler, $\mathbf{K}$. The standard deviation used to randomize the strengths of all directional coupler present in the system, $\mathbf{K_{std}}$. This is included to simulate variations in coupling ratios stemming from fabrication errors. The length every ring resonator in the system has before additional randomization, $\mathbf{L}$. The standard deviation used for the designed pair-wise length randomization, $\mathbf{L_{rand}}$. The standard deviation used for the individual ring length randomization, $\mathbf{L_{std}}$, included to simulate fabrication errors. The loss parameter for the waveguides in DB cm^{-1}, **DBloss**. The effective refractive index experienced by light traveling through a waveguide on the chip, $\mathbf{N_{eff}}$. The value 1.505 is chosen due to the properties of the TriPleX silicon-nitride platform [29].

As part of the simulations, the transmission matrix representing a tPUK system is given an optical pulse as input. The pulse, $E_{in}(\lambda)$, is modeled as a normalized Gaussian with a center wavelength of 800 nm and a FWHM of 13 nm. This mimics the properties of the laser source in the lab. To prevent the model from producing nonphysical values, the value $\mathbf{K}$ is bounded between 0 and 1 after randomization for every directional coupler. Additionally, the resonator lengths are all lower bounded at 0. The simulations are further verified to be correct by setting the loss parameter, **DBloss**, to 0 and checking for energy conservation.

The output field is simulated for all three system sizes. The simulation results can be viewed in figure 4.2. The spectra shown are those belonging to the throughput output of the systems. Mathematically, the transformation applied while light travels to the throughput output can be represented by a multiplication of the transmission matrix element t_{00} with the input pulse, $E_{in}(\lambda)$. The simulation parameters used are chosen to resemble the designed parameters of the tPUK chips. That being: $\mathbf{L}$ = 2250 µm, $\mathbf{L_{rand}}$ = 20 µm, $\mathbf{L_{std}}$ = 50 nm, $\mathbf{K}$ = 0.5, $\mathbf{K_{std}}$ = 0.05 and **DBloss** = 0.8 dB cm^{-1}.

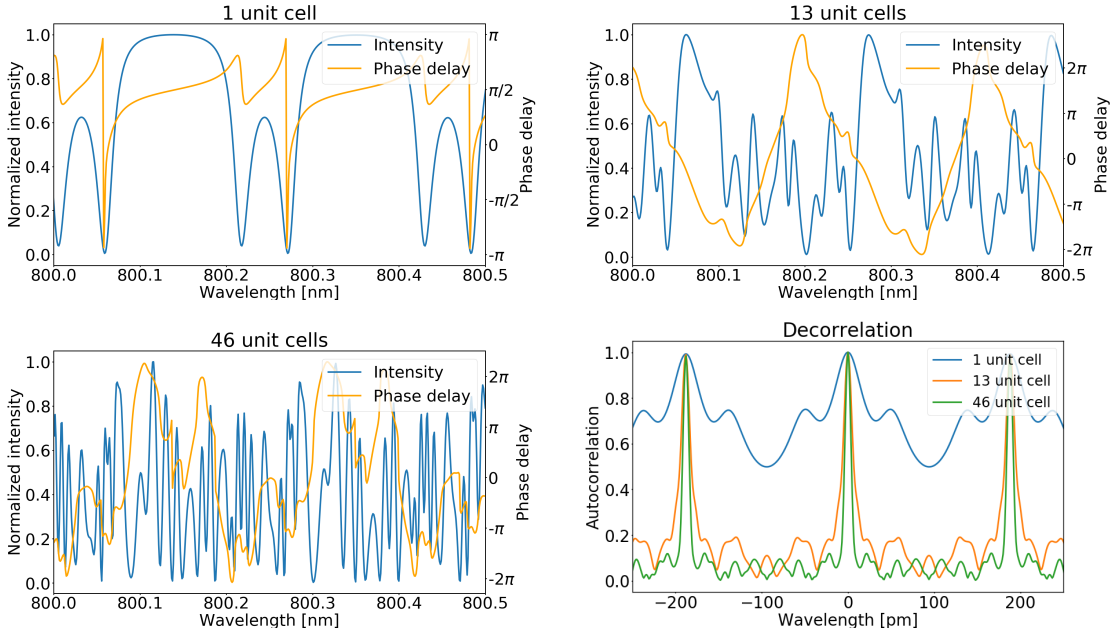

Figure 4.2: In this figure three subplots are shown that feature the throughput output power spectrum and phase spectrum of every simulated system size. For the systems consisting of multiple unit cells the wrapped phase is plotted for clarity. The linear phase gradient stemming from dispersion is also removed. Also included in this figure is a subplot that shows the simulated decorrelation for every system size.

As figures 2.4 and 4.2 show, a single ring resonator unit cell on its own does not perform a tPUK like transformation. Because of the periodicity of the output spectrum and the relatively broad spectral features (≈ 20 pm resonances), it will not be hard to copy its response with a pulse shaper. Furthermore, a single unit cell will not distribute input evenly across both spatial outputs. Approximately 68% of the total output intensity is distributed to the throughput output. This also means that there is already a large ratio between the non-linear intensities of the two spatial outputs before shaping the input. In a method such as tPEAC, one would ideally start with a 1 to 1 output ratio, so the receiving party can easily interpret the information they are sent.

Moving towards the larger systems, they clearly show that the output spectra become increasingly more random-looking as the number of unit cells is increased. This is especially noticeable for the power spectra. The average width of the spectral features also seems to decrease for increasingly larger systems. These observations can both be understood by studying the decorrelation length for every system. This length is the wavelength shift needed for the transmission of the tPUK system to become uncorrelated with itself.
To calculate the decorrelation length, we first take the auto-correlation of the tPUK's

throughput transmission matrix element t_{00}. This auto-correlation can be defined as:

$$C(\Delta\lambda) = \langle t_{00}(\lambda + \Delta\lambda) t_{00}(\lambda)^* \rangle \tag{4.1}$$

Where $\langle ... \rangle$ denotes the expectation value over all wavelengths. The correlation is then finally normalized by its maximum value, C(0). The calculated auto-correlation plots will show a correlation peak in their center where the wavelength shift approaches 0. The FWHM of this peak is then the decorrelation length.

The bottom-right subplot of figure 4.2 shows a plot of the simulated auto-correlations centered around $\Delta\lambda = 0$ for all three tPUK systems. The plot shows a few interesting features. Firstly, the width of the center correlation peak decreases as the number of unit cells in the system increases. As stated earlier, the effects of this shorter decorrelation length are observed clearly in the power spectra of the larger systems. Another interesting result is that there are more correlation peaks present besides the center peak. In the plotted graph, secondary correlation peaks are visible and if the x-axis would be expanded further even more peaks would be visible. These peaks can be explained by the fact that the difference in ring lengths designed into the tPUK systems is still relatively small, $\mathbf{L_{rand}}/\mathbf{L} < 0.01$. The FSR of a ring resonator with length $\mathbf{L}$ is 189 pm according to eq. 2.6. This is also the wavelength shift where the secondary peaks are observed in the auto-correlation plot.

From the performed simulations we thus predict that no tPUK-like output spectrum will be observed for a single unit cell system. Additionally, the larger systems are predicted to possess random-looking output spectra but featuring a clear periodicity on the order of the mean ring length FSR.

4.2 Experimental characterization

To investigate the predictions made from previous simulations, the tPUK chips were characterized experimentally. To characterize the ring resonator systems present on the tPUK chips the output power spectra of these systems were measured using a Michelson interferometer and Fourier interferometry. See section 3.1.3 for more experimental details about the Michelson interferometer.

4.2.1 Single unit cell system

As stated before, the ring resonator system consisting of a single ring resonator pair is not expected to produce an output power spectrum corresponding to that of a tPUK. It is however still interesting to study its output spectrum. Firstly, the single unit cell system is a relatively small system from which the losses are expected to be relatively small. Approximating the length of waveguide traveled by light as $\mathbf{L} * 1.5 + \text{Chiplength} \approx 0.4$ cm+1.6 cm = 2 cm. The loss is roughly expected to be $2 * 0.8\text{dB} = 1.6\text{dB}$. Because of the low losses, the pulse's sech^2 shaped envelope is expected to be mostly unaffected by the ring resonator system. Thus a roughly sech^2 shaped power spectrum is expected to be measured, also showing the resonances of the double-ring resonator unit cell. The auto-correlation interferogram, as well as the full power spectrum, can be viewed in figure 4.3.

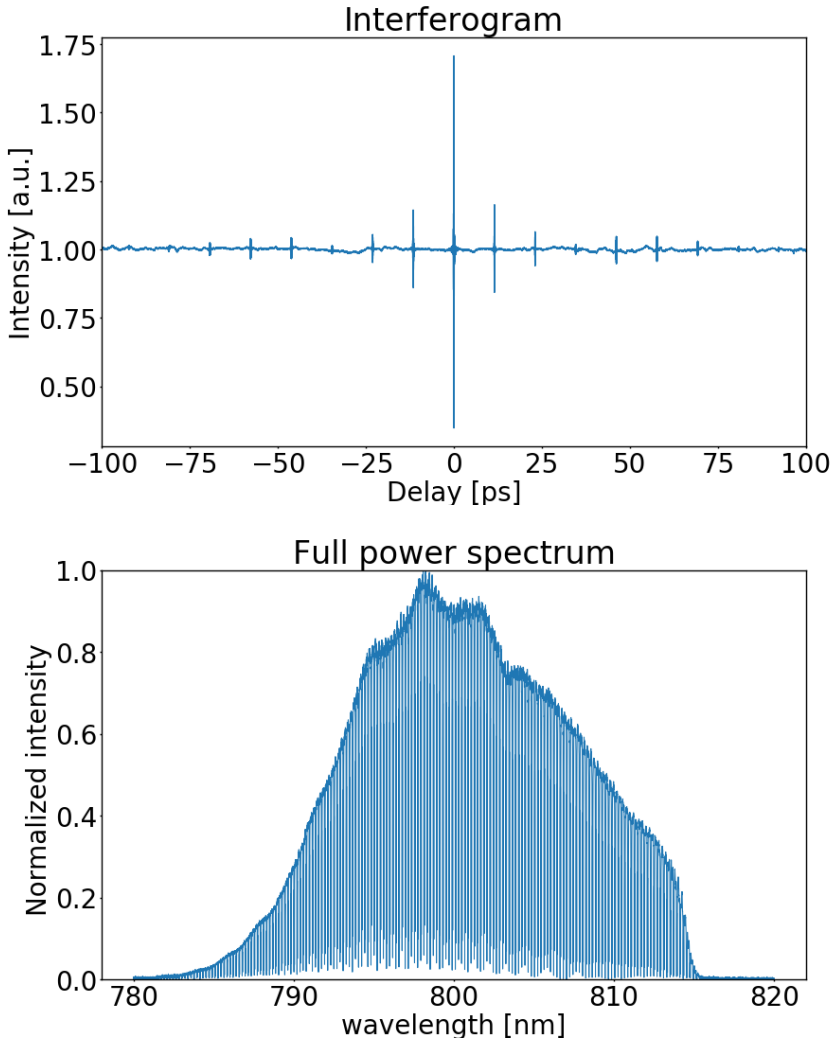

Figure 4.3: *Top* : A section of the measured interferogram centered around the zero delay point. The full interferogram ranges from around -200 ps to 580 ps. The intensity signal plotted is plotted by the mean signal intensity. *Bottom* : The measured power spectrum in its entirety. The range of delay allows for a measurement of the power spectrum with a spectral resolution of $\approx$ 2.6 pm.

The plots displayed in figure 4.3 already show some features that can be used to judge the quality of the interferometer as well as determine some properties of the single unit cell design. Using the maximum and minimum intensity of the interferogram, the fringe visibility, $V = (I_{max} - I_{min})/(I_{max} + I_{min})$, of the interferometer, can be obtained. For the interferogram of figure 4.3 the following visibility is found: V = 0.66. An ideal interferometer would have a fringe visibility, V, of value 1. The less than ideal visibility is due to setup practicalities such as beam splitter imperfections and small beam direction and position mismatches. While being less than ideal the achieved visibility proved to be sufficient for accurate acquisition of the power spectra.
The periodic spacing of the peaks in the measured auto-correlation provides a way to experimentally estimate the effective refractive index, $\mathbf{N_{eff}}$, experienced by light propagating through the chip. The 11.5 ps periodic spacing of the auto-correlation peaks corresponds to the extra optical path traveled through a ring resonator. Assuming a ring length of ap-

proximately 2250 µm, the effective refractive index can be calculated from the expression for optical path length: $\Delta OPL = \mathbf{L} \times \mathbf{N_{eff}}$, and the delay experienced: $\Delta t = \Delta OPL/c$. With c denoting the speed of light. Thus an effective refractive index of $N_{eff} = 1.53$ is found. This is very close to the value assumed for the simulations. The plot of the full power spectrum shows that the pulse envelope is pretty well preserved under propagation through the chip. This is especially evident on the shorter wavelength side of the pulse. The distortion of the pulse envelope towards the longer wavelengths is mostly due to the transmission properties of a half-wave plate positioned before the chip.

The single unit cell system can be simulated with only two length parameters. Therefore, the small number of input parameters can be fitted in order to match the output spectrum produced in simulations with the output spectrum retrieved experimentally. Doing so enables more accurate measurements of interesting chip properties such as loss per cm, **DBloss**, and the mean coupling constant, **K**. Most importantly it allows for a measurement of the length difference between two ring resonators that is solely caused by fabrication errors. This measurement provides us with a better estimation of the scale of the fabrication errors generally encountered throughout the tPUK systems. As mentioned before, every chip is designed with their own coupling constant. Figure 4.4 shows the throughput power spectrum for the chip designed with 50/50 directional couplers, along with the fitted simulation output.

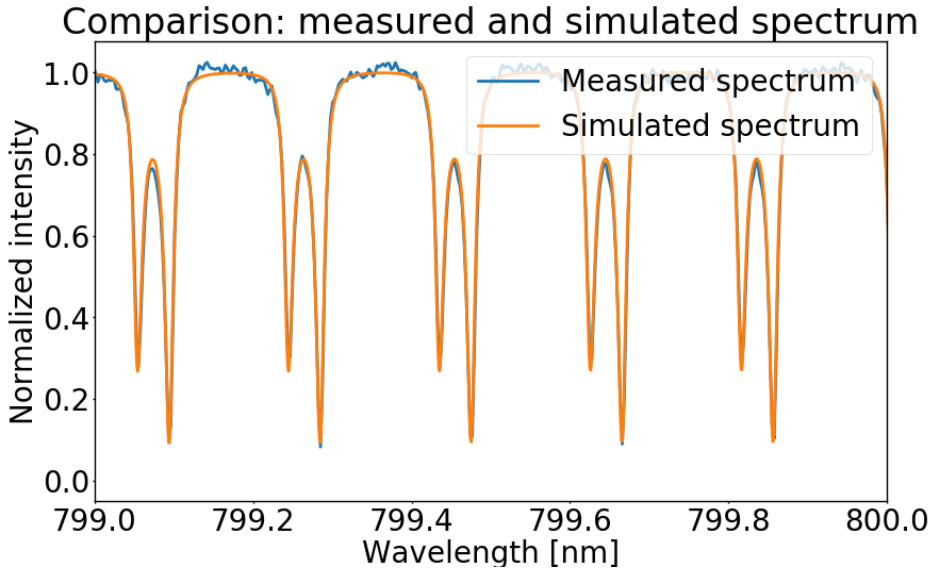

Figure 4.4: The measured throughput power spectrum of a single unit cell ring resonator system compared with the best fitted simulation result.

Before fitting the simulated output, the measured output power spectrum is corrected for the pulse envelope. This allows for more accurate fitting as the model solely describes the spectral features resulting from the tPUK unit cell and not the other optical components present in the setup. The fitting was performed in two steps. First, the input parameters of the unit cell model were fitted manually to get an accurate looking fit. Then the parameters were fitted with more precision individually using a least-squares fitting method.

$\mathbf{K_d}$	$\mathbf{K}$	$\mathbf{\Delta L}$
0.4	0.25	25 nm
0.5	0.35	124 nm
0.6	0.38	10 nm

Table 4.1: The $\mathbf{K}$ and $\mathbf{\Delta L}$ input parameters found for each $\mathbf{K_d}$. Additionally, every chip was found to have the same waveguide loss parameter of 0.9 dB cm^{-1}.

Table 4.1 shows the $\mathbf{K}$ and $\mathbf{\Delta L}$ input parameters found for three chips, each with a different designed intensity coupling constant, $\mathbf{K_d}$. With $\mathbf{\Delta L}$ being the length difference between the two ring resonators in the single unit cell. It is immediately noticeable that all measured intensity coupling constants, $\mathbf{K}$, are significantly lower than what they were designed to be. The discrepancy observed is most likely due to inexperience with the fabrication of directional couplers that function around 800 nm. The smaller coupling constants mean that all fabricated ring resonators on the chips will feature resonances with smaller spectral widths. As a consequence of this, there could be less overlap of resonances between different ring resonators. With less overlap, a system might need more unit cells before showing a tPUK-like response. The discrepancy in intensity coupling ratio will have to be taken into account if new chip designs are to be fabricated around 800 nm.

As stated in table 4.1, two of the fabricated chips show a ring resonator length difference, $\mathbf{\Delta L}$, in the order of tens of nanometers. A standard deviation of 50 nm for the individual randomization of the ring resonator lengths does seem a reasonably accurate estimation. This standard deviation would also allow the occasional ring resonator fabricated with a larger length difference, which is also seen in table 4.1. Considering an average ring resonator length of 2250 μm, a 50 nm fabrication error would correspond to an error of approximately 22 ppm. In previous work studying tPUKs, the ring resonator model also used in this research showed that a fabrication error of 25 ppm would already lead to completely decorrelated chip responses for systems consisting of 50 unit cells [10]. The model does not take into account factors such as wavelength dependent coupling constants or wavelength dependent propagation losses. These additional factors could make fabrication errors even more critical.
As a final note, the waveguide loss parameter was found to be 0.9 dB cm^{-1} for each chip. This corresponds pretty accurately to the 0.8 dB cm^{-1} value reported by LioniX.

4.2.2 Multiple unit cell systems

Moving on from the single unit cell system, the systems consisting of multiple unit cells were also characterized experimentally. As simulations showed earlier, these systems are expected to show tPUK-like behavior. To study the effect of fabrication errors, the throughput power spectrum of a tPUK system is compared to the throughput output of the tPUK system's exact copy, present on the same chip. As is part of the systems' intended functionality, their output spectra are not easily reproduced exactly with simulations. Therefore the measured output spectra can only be compared to simulations in a general manner. General properties of the measured power spectra, such as spectral feature width or returning periodicities, can still be compared. Figure 4.5 shows sections of the measured throughput power spectrum for systems consisting of 13 and 46 unit cells.

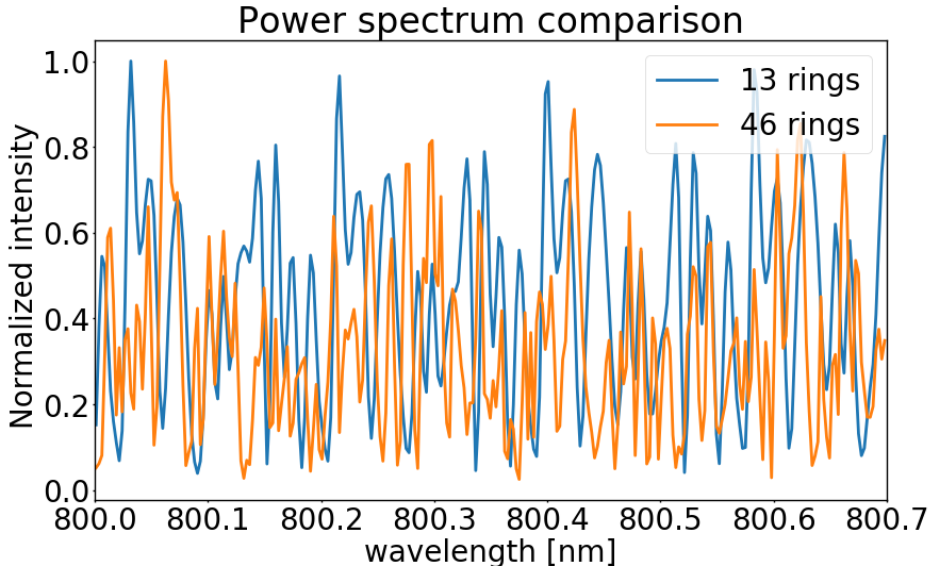

Figure 4.5: Shown here is a section of the throughput power spectra measured for tPUK systems consisting of 13 and 46 ring resonator unit cells.

The output spectra shown in figure 4.5 appear at first glance to be in line with what was predicted by simulations. Adding to this, the spectral features shown in these spectra appear more narrow as well ($\approx$ 10pm). It seems the 46 cell spectrum has slightly narrower features than the 13 cell spectrum. It is however difficult to tell as the spectral resolution of the interferometer starts to become troublesome here. Many peaks observed in the 46 cell spectrum consist of just one or two data points. There might be even narrower features present in the 46 cell spectrum that we are not able to observe. Something making the spectra less random looking is the fact that there is still a clear periodicity visible in the spectrum belonging to the system of 13 unit cells. This periodicity again corresponds to the FSR of the mean ring length ($\approx$ 189pm). This periodicity does not appear clearly in the plotted section of the 46 cell spectrum. However, it is still observed in some other parts of the spectrum.

As discussed earlier it is of great interest to compare the output power spectrum of a system to the one measured for the system's copy. Figure 4.6 shows such a comparison of the spectra of the 13 unit cell systems present on the 50/50 coupling ratio chip. The spectra shown in the figure do look noticeably different. However, they do not appear totally uncorrelated as can be gathered from the shared peaks present in the spectra. To quantify the similarity between the two spectra we can take their cross-correlation. As no phase information is measured, only the power spectra cam be correlated. For this the Pearson correlation coefficient (PCC) is used [43]. The Pearson correlation coefficient can be defined as follows:

$$\gamma = \frac{\sum_i (x_i - \bar{x})(y - \bar{y})}{\sqrt{\sum_i (x_i - \bar{x})^2}\sqrt{\sum_i (y - \bar{y})^2}} \tag{4.2}$$

Here x and y denote the two 1D data sets correlated with each other. x_i denotes the i$^{\text{th}}$ element of data set x and $\bar{x}$ the mean value of data set x. The same is true for y_i and $\bar{y}$. The Pearson coefficient is a measure of the linear correlation between two data sets. It can range between the values -1 and 1. With -1 being a perfect anti-correlation and 1

being a perfect correlation.

Correlation coefficients of 0.37 and 0.17 are found for the 13 unit cell system and 46 unit cell system respectively. These values indicate only a weak correlation between two system copies. Especially the 46 unit cell system shows a very weak correlation. Thus it seems that manufacturing errors indeed become more critical when copying ever-larger tPUK ring resonator systems. The actual correlation coefficients might in reality be even lower. The limited resolution of the interferometer provides a certain baseline of correlation as uncorrelated data points are averaged to correlated data points. With this being the case, the most important result is the downward trend in correlation coefficients and not their precise value.

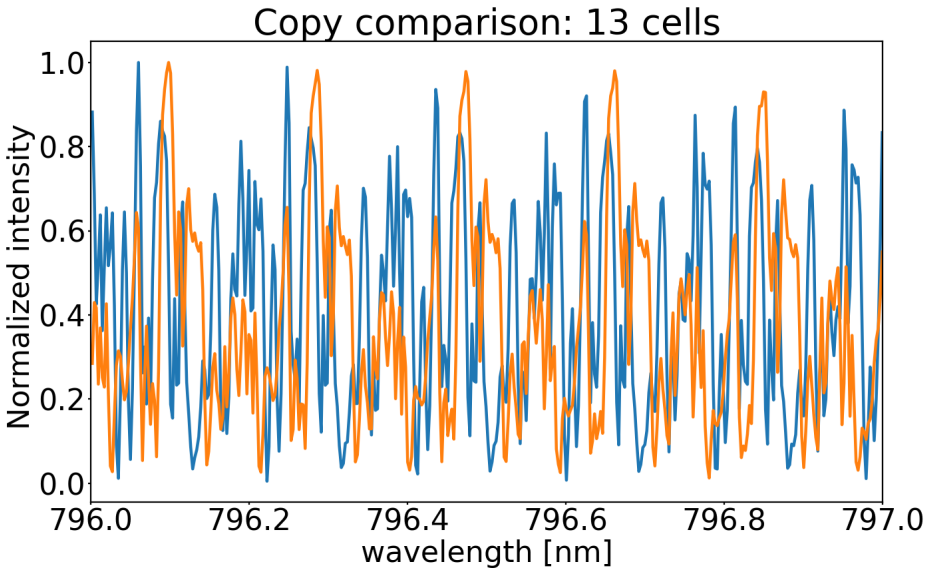

Figure 4.6: This figure shows a section of the throughput power spectra measured for two tPUK systems consisting of 13 unit cells, designed to be exact copies of each other. Each trace color represents a different system.

Apart from the random-looking and weakly correlated output spectra, the larger tPUK systems also show a problematic transmission characteristic. Their transmission losses are quite high. Transmission losses of 10.3 dB and 18.8 dB were measured for the 13 cell systems and 46 cell systems respectively. These losses were measured by comparing the total output power in both spatial outputs of a system to the input power using a power meter. As the output power is evenly distributed across both system outputs, the effective transmission loss is double that of the total transmission loss mentioned earlier. When working with optical pulses the chips can only be operated with input powers of tens of milliwatts. High transmission losses can thus easily lead to output powers lower than 1 mW. This can be a serious obstacle for non-linear detection of the chip output in schemes such as tPEAC.

4.3 Alternative unit cell design

The knowledge gained in studying the current generation of tPUK chips can be incorporated when designing new tPUK chips. Even though the systems designed on the current chips show transmission responses that are already very random-looking and uncorrelated, there are still some points of improvement. The most important point of improvement being the chip losses. Effective ways of lowering transmission losses would be to use smaller tPUK systems that still possess tPUK-like transmission responses. Additionally, smaller tPUK systems would leave more free room on the chip and allow for the waveguide bends present in the tPUK system to be designed with larger bending radii and thus, again, lower propagation losses. An effective way to reduce the system size would be to reduce the number of unit cells. Doing so whilst still conserving the tPUK-like transmission characteristics could be achieved by coming up with a new unit cell design.

A possible design choice is to include more ring resonators into a single unit cell. An interesting way of doing this is by introducing nested rings/loops. See figure 4.7 for a sketch of a possible design featuring two smaller nested rings. By introducing the two nested rings the transmission response of the unit cell is made drastically more complex. Intuitively this can be understood by considering that by adding these nested rings, a large number of new forward paths and loops have been added to the unit cell. As stated in theory section 2.2, the current designs feature three different forward paths to the throughput output and three loops possible in the unit cell. In contrast, the new design features 21 forward paths to the throughput output and 28 possible loops. To more accurately predict the transmission response of the new unit cell design simulations are required. For this purpose, the model used for the current unit cell design, as described in section 2.2, is adapted for this new proposed nested ring unit cell design. Due to the size of the mathematical expressions encountered, the derivation of the new unit cell model is left out of this thesis. Even though the new model needs to take in a much larger number of forward path gains and loop gains, it still works with almost the same input parameters. The only addition is a parameter to set the mean length of the smaller nested rings.

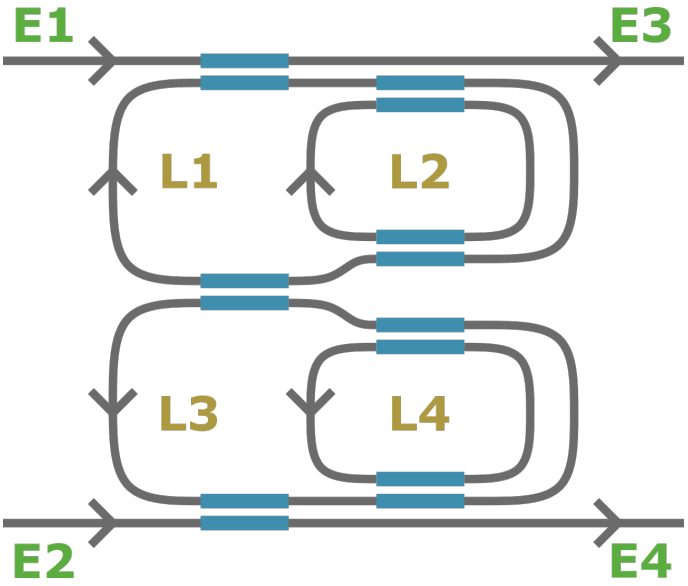

Figure 4.7: The proposed nested ring unit cell design. Two new smaller rings are added inside the two larger rings. Light can travel to the nested rings through newly added directional couplers.

To compare the characteristics of this new unit cell design with the current design, simulations were performed for systems with 15 unit cells with the same input parameters as the simulations mentioned in subsection 4.1.1. The mean length of the small rings was chosen to be 0.6 times that of the larger rings. The left section of figure 4.8 shows a portion of the throughput spectrum simulated for a 15 unit cell tPUK system using the new unit cell design. Its spectral features are roughly as narrow as one would expect for the current design. A large difference however is the fact that there is no clear periodicity visible anymore. With the addition of the nested rings, the new unit cell design contains ring resonators with significantly different ring lengths. Because of this the periodicity that was due to the shared FSR is no longer present in the output spectrum. This can also be seen in the plot in the right section of figure 4.8. The plot shows the correlation of the system output with itself, as described by equation 4.1.

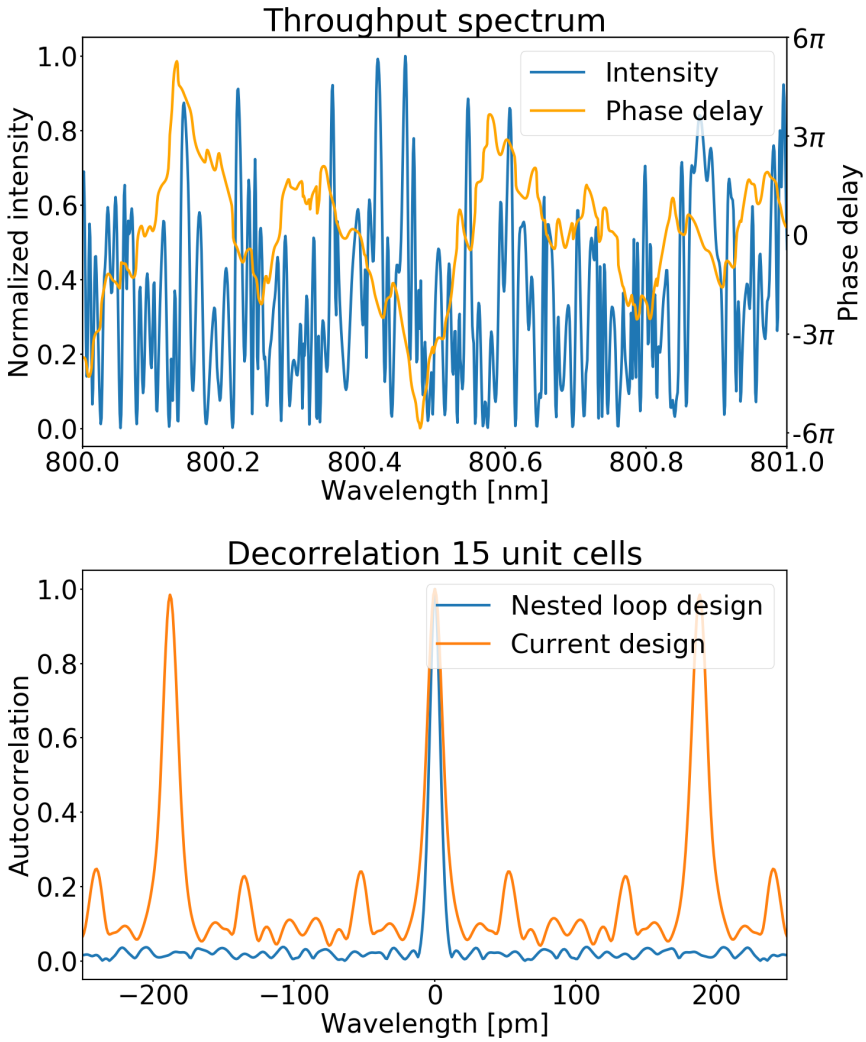

Figure 4.8: *Top*: A section of the throughput spectrum simulated for the proposed nested ring design. *Bottom*: A plot comparing the autocorrelation of the spectrum for the new design and current design for a certain wavelength shift.

Simulations also provide an insight into how many newly designed unit cells might be needed for a system to show tPUK-like qualities. One of these tPUK qualities is a random-looking transmission response. As stated before, a random-looking transmission response is generally obtained for systems with a short decorrelation length. Thus we need to investigate how the decorrelation length decreases with the number of unit cells. The left section of figure 4.9 shows a plot of this decorrelation length as a function of the number of unit cells. The comparison shown in the figure indicates that the newly proposed designed decreases to a small decorrelation length slightly quicker than the current design.

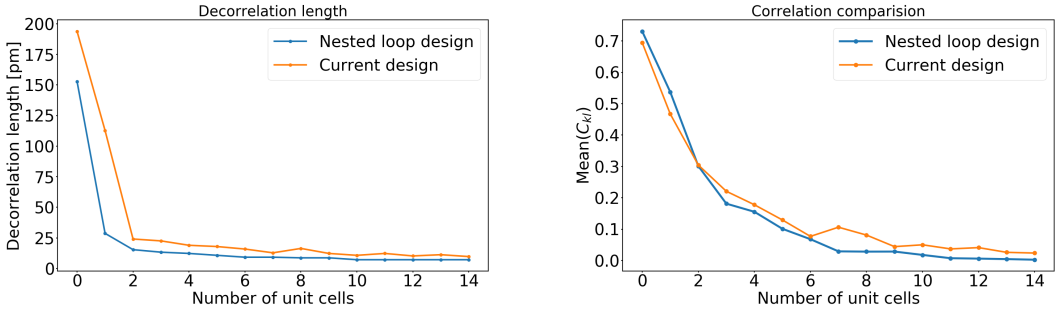

Figure 4.9: *Left*: A plot of the average decorrelation length simulated for the current design and the new design. The decorrelation length plotted corresponds to the FWHM of the central peak in the auto-correlation plot. *Right*: A plot showing the mean cross-correlation coefficient found per number of unit cells, averaged over 30 values, for both unit cell designs. Both designs feature very low cross-correlation coefficients for systems larger than 10 unit cells.

Another important tPUK property is of course that it is infeasible to copy a tPUK. Thus a copy of a system should not show the same transmission response as the original system. To investigate this, a copy can be simulated and its output spectrum cross-correlated with that of the original system. The cross-correlation coefficient that is used for this is defined as follows:

$$C_{kl} = \left| \sum_{\lambda} \exp\left[-i \arg(t^{k}_{00}(\lambda))\right] t^{l}_{00}(\lambda) \right|^2 \Bigg/ \left(\sum_{\lambda} \left| t^{l}_{00}(\lambda) \right| \right)^2 \tag{4.3}$$

Where C_{kl} is the cross-correlation coefficient of tPUK systems k and l. Also t^{k}_{00} and t^{l}_{00} denote the throughput transmission matrix elements of systems k and l. The value of this cross-correlation coefficient ranges from 0 to 1. This correlation coefficient is specifically chosen because it has a useful physical interpretation. It can be interpreted as using time-domain wavefront shaping on output 0 of system k and subsequently measuring the relative response of system l, at t = 0, for that same wavefront.

The right section of figure 4.9 shows the mean cross-correlation coefficient found for both the new unit cell design and the current unit cell design. This mean value is found by averaging over 30 simulated system copies. The figure shows that both designs require 10 or more unit cells to be considered unclonable. However, it must be noted that the alternative unit cell design is much more consistent with respect to the value of its cross-correlation coefficient. For a system of 15 unit cells both designs, old and new, feature a small cross-correlation value of approximately 0.024 and 0.004 respectively. The standard deviations found are 0.024 and 0.005 respectively. The standard deviation found for the

current design is more than five times as large as the one found for the new design. Practically this means that protection against key imitation attacks is less consistently provided by the current design compared to the new design. An attacker could fabricate a large number of copies and have a chance to find one that matches the original.

It can be concluded from the performed simulations that we need about 10 to 15 of the new unit cells to fabricate a promising tPUK system. As indicated by the results in figure 4.9, such system sizes will feature a short decorrelation length and will be difficult to copy. While the current unit cell also features a low cross-correlation and decorrelation length for such system sizes, it does still clearly show periodicities in its output spectrum. It was shown experimentally that these periodicities are still not fully gone when studying the throughput of a 46 unit cell system. In contrast a comparably sized system consisting of the new unit cell design does not show these periodicities in its output spectrum and is more consistently unclonable.

4.4 Summary

The fabricated tPUKs show transmission properties that are in accordance with what is predicted by simulations. All fabricated chips do however feature an intensity coupling ratio lower than the designed value. The measured throughput spectra of the fabricated larger tPUK systems display intricate features and are already quite random-looking. However, periodicities still appear in the measured spectra that prevent them from being truly random-looking. Large tPUK systems are also shown to have high transmission losses, making non-linear detection of their output more difficult. To solve this, future generations of tPUK chips could be produced with a new unit cell design featuring nested rings. This new design would allow for systems consisting of around 15 unit cells to possess the required tPUK qualities. These include a truly random-looking transmission spectrum without periodicities and being consistently infeasible to copy.

5. tPUK demonstration

This chapter provides a proof-of-concept demonstration of the tPUK nature of the ring resonator chip samples. Using the pulse shaper and non-linear detection setup, it is possible to perform feedback-based temporal wavefront shaping on the chip input. This chapter will explain the shaping algorithm used as well as describe the experimental conditions of the shaping process. The results from the temporal shaping efforts are also shown in this chapter.

5.1 Feedback-based temporal wavefront shaping

The goal of temporal wavefront shaping is to find the optimal phase for every controlled input frequency mode. The transmission matrix describing the shaping sample is often not known beforehand. In such a case an iterative method has to be used to converge towards the optimal shaping phases. Such a method relies on a feedback signal that measures the achieved enhancement for every shaping iteration. There exist many iterative wavefront shaping algorithms, each with its own advantages and drawbacks. As described earlier in chapter 4, the larger ring resonator systems suffer from significant transmission losses, 10.3 dB and 18.8 dB for the 13 and 46 cell systems respectively. Due to these losses, low signal-to-noise ratios are expected. An iterative shaping algorithm particularly suited for such conditions is the partitioning algorithm. Furthermore, it is robust against temporal variations of the shaping sample and is easy to implement [20, 34, 44, 45].

Before starting the partitioning algorithm, the SLM or pulse shaper that is used is instructed with a random phase for every control channel (pixel). This is done to prevent a local optimum from occurring at the start of the algorithm. In every shaping iteration of the algorithm, the N controllable channels of the pulse shaper are randomly divided into two partitions of equal size. The phases for the channels in one of these partitions are then shifted by an amount ranging from 0 to 2π, in small steps. During this process, the phases for the other partition remain the same. For spatial wavefront shaping, the intensity measured in the shaping region will behave as follows:

$$\int I(\Phi)dt \sim A + B\cos(\Phi - \Phi_0) \tag{5.1}$$

Here Φ is the phase of the shaper controls in one of the partitions and Φ_0 is the optimal phase [44]. The cosine is fitted to retrieve the optimal phase of the partition. After this optimal phase is set the algorithm moves on to the next iteration and divides the controls into two new partitions. The optimal phase is eventually found for every controllable channel by repeating over many iterations.
For time-domain wavefront shaping a non-linear feedback signal is used. The square of the intensity is measured, which behaves as:

$$\int I^2(\Phi)dt \sim \big(A + B\cos(\Phi - \Phi_0)\big)^2 \tag{5.2}$$

This is the model used for fitting the optimal phase.

5.2 Shaping results

Temporal wavefront shaping was performed on the chip designed with an intensity coupling ratio of 0.6. Shaping was performed for all ring resonator system sizes. The non-linear feedback signal is compensated for output intensity fluctuations in all shaping efforts presented in this section. In these shaping efforts, a distinction can be made between shaping on one system output or on both system outputs. When shaping on one system output, one only uses the non-linear signal at one output as feedback. When shaping on two outputs of a system, one uses the ratio between the non-linear intensities at both outputs as feedback for the shaping algorithm. Shaping iterations are performed with a phase stepping speed of five phases per second.

First presented here are shaping attempts that utilize only one of the chip outputs for feedback. These measurements were all taken with a chip input power of 20 mW. The measured enhancement clearly shows what level of absolute non-linear enhancement the setup can achieve for every tPUK system size. Figure 5.1 displays the measured non-linear enhancement of all three systems for every shaping iteration. The enhancement displayed is calculated as the the ratio between the non-linear signal measured for that iteration and the non-linear signal for the randomly shaped start wavefront.

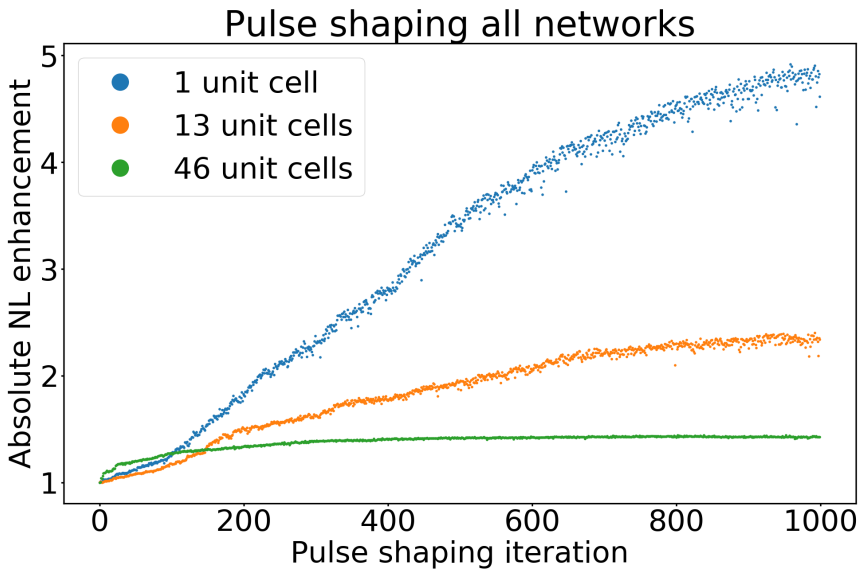

Figure 5.1: Shown here is the absolute non-linear enhancement measured for every system size over 1000 shaping iterations. All systems were shaped with the same chip input, 20 mW. Achieved enhancement: 1 unit cell: 25, 13 unit cells: 5, 46 unit cells: 2.

Figure 5.1 shows that the absolute non-linear enhancement achieved decreases significantly for the larger systems on the chip. This has two major experimental causes. Firstly, the starting non-linear output intensity is considerably lower for these larger systems due to their significant transmission losses. Naively one assumes the absolute non-linear intensity of the output to be unimportant as the non-linear enhancement should theoretically improve linearly when shaping. However, the detection of the non-linear detector decreases at low intensities. Furthermore, the detector also still has a small linear absorption. In the limit of low signal intensities, this linear component of the detector signal becomes significant with respect to the total detector signal (non-linear + linear). Shaping only improves the non-linear intensity, so this linear offset may substantially decrease the final value found for the enhancement.

Another thing to be considered is the fact that the larger systems apply a much more complex transformation on the input signal than the single unit cell system. Because of this, the pulse shaper has more trouble in compensating for the transformation of the larger systems. As discussed in subsection 3.1.4, the pulse shaper only has a limited shaping resolution (64 pm). As is discussed in chapter 4, the larger tPUK system feature a very small decorrelation length (< 10 pm). This means that roughly only one of six spectral features present on a single shaping pixel is effectively shaped. An additional practical limitation is the fact that a pulse shaper can only add a single phase delay to a controllable frequency component. Consider that a single ring resonator has a round-trip delay of 11 ps. Light passing through a ring may be delayed by one round-trip length or even multiple, as can be seen in figure 4.3, showing the output auto-correlation signal. Effectively, a single frequency component is split into multiple parts with different delays. For a system consisting of many unit cells, the number of possible delays increases dramatically. Consequently, the single frequency component is smeared out in the time domain between a minimum time delay and a maximum time delay. By time-domain wavefront shaping, we can only compensate for one of these many delays. Typically, the delay component compensated by the pulse shaper is the one with the largest amplitude. The fact that only a single delay can be properly compensated means that the other components will not necessarily interfere constructively into an output pulse.

The initial shaping results show some of the experimental limitations currently present in the setup. The second part of the shaping results focuses on temporally shaping the input of a system while using the non-linear signal from both system outputs as feedback. By measuring the non-linear intensity at both outputs, one can use their ratio as the feedback for the shaping algorithm and increase that ratio further. The ability to improve this ratio is exactly what is required for security applications like tPEAC. In tPEAC wavefronts belonging to the H_0 and H_1 groups are able to skew the output ratio one way or the other, respectively meaning a 0 or a 1. To be able to use both outputs for feedback while using only one non-linear detector, we need to move the output coupling lens in every shaping iteration to switch between the system outputs. As the lens is placed on an electronically controlled piezo stage, this switching can be automated.

Figure 5.2 shows two attempts at shaping the non-linear intensity ratio between the two outputs of a ring resonator system consisting of 13 unit cells. The left of figure 5.2 shows an attempt where only the non-linear signal in the target output is used as feedback for the shaping algorithm. The figure clearly shows that when attempting to improve the non-linear signal at one of the two outputs the non-linear signal at the other output is also improved. An effective way for the pulse shaper to improve the output signal is to remove the general dispersion introduced by the waveguides on the chip. This general

dispersion is experienced by light traveling to both outputs. Thus by compensating for this dispersion, both output signals are improved. The right of figure 5.2 shows a shaping attempt where both output signals were used as feedback for the shaping algorithm. In this case, the shaper can specifically optimize the ratio between the two outputs in favor of the target output. Instead of compensating for general dispersion, the shaper is now specifically trying to compensate for the delays introduced by the ring resonators in the tPUK system.

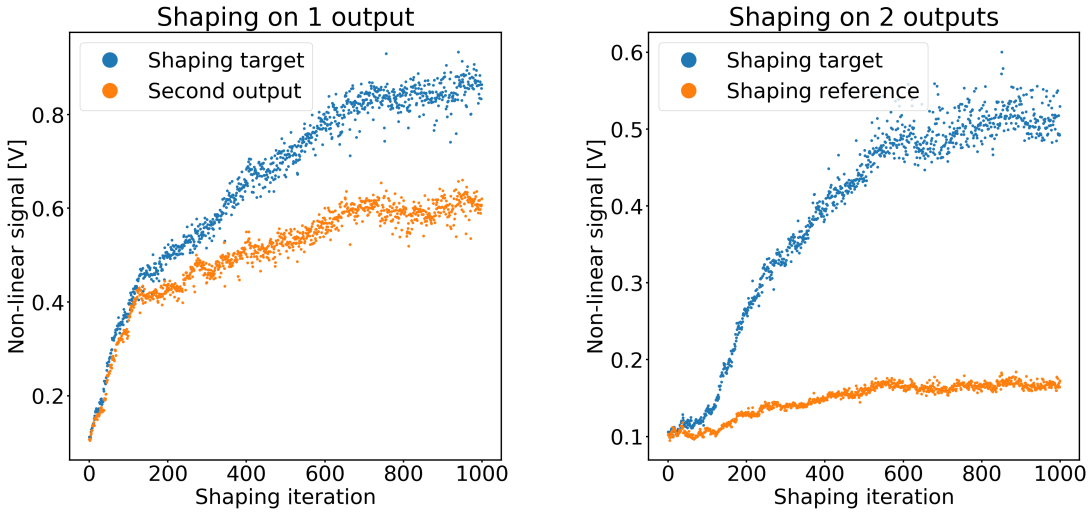

Figure 5.2: *Left*: A plot of the non-linear detector signal for two outputs of the same system consisting of thirteen unit cells. Only the non-linear intensity in the target output is used as feedback for the shaping algorithm. *Right*: A plot of the non-linear detector signal for two outputs of the same system consisting of thirteen unit cells. The ratio of the two outputs is used as feedback for the shaping algorithm. The ratio is skewed in favor of the target wavefront.

As figure 5.2 shows, we can successfully create a non-linear output signal ratio of factor 3 for a 13 unit cell system. The optimal phase settings found in this process do not translate well to other 13 cell systems. When using the optimal phase settings belonging to a specific system on another system of the same size, no non-linear output ratio is observed that is significantly larger than that observed for a randomly shaped input wavefront. This is however only true for ratio shaping. By shaping on one output and thus mostly compensating for general dispersion, one can give the found wavefront as input to a same-sized system and get a significant improvement in the non-linear intensity signal at the output.

Shaping on two outputs was also attempted for a 46 unit cell system but unsuccessfully as of yet. Although improving the non-linear signal of a single output is certainly possible for these systems, the achieved signal to noise ratio has not allowed for ratio shaping. To improve this signal-to-noise ratio, improvements can be made to the pulse shaper as well as the non-linear detection method. Such suggestions are treated with more detail in chapter 6.

6. Discussion

In this chapter, some of the experimental results are discussed as well as experimental difficulties encountered while obtaining them. The discussion highlights some points where the experimental setup can be improved.

6.1 Interferometer design

As shown in chapter 4, the integrated tPUK samples are characterized experimentally using a Michelson interferometer. Such an interferometer is only able to obtain the output power spectrum of the samples. However, the phase spectrum is also of great importance when studying tPUKs. As discussed in theory section 2.1, an essential transmission characteristic of a tPUK is to provide a seemingly random phase delay to different frequencies. A measurement of the power spectrum, where we assume a random-looking power spectrum corresponds to a random-looking phase spectrum, only gives an indirect measurement of these random phase delays. To also be able to measure a sample's phase spectrum, we need to use an interferometer design capable of performing a cross-correlation between the chip input signal and output signal.

An interferometer design capable of performing this cross-correlation is the Mach-Zehnder interferometer. This actually was the interferometer design first built in the lab before the Michelson design. A Mach-Zehnder interferometer was built where the tPUK samples were placed in the sample arm. The reference arm could be scanned using a HeNe referenced linear translation stage. Unfortunately, the interferometer suffered from instabilities in the optical path length of each interferometer arm. Because of these instabilities, accurate measurement of the tPUK samples' output spectra could not be performed. The current Michelson interferometer is protected against path length instabilities by use of a HeNe reference. In the Mach-Zehnder design, it is not possible to use the HeNe laser source as a reference for both arms as one of the arms includes the tPUK sample. To be able to measure the phase spectrum in the future, a method called the 'phase shift method' could be tried. This method uses amplitude modulation of the input signal to eventually determine the output's phase spectrum. It is further described in the appendix A.1.

6.2 Pulse shaper

The 4f pulse shaper present in the lab has a limited shaping resolution as well as a limited time window in which it can shape. Due to these limitations, the pulse shaper is not able to compensate well for the complex transformation the larger tPUK systems apply on an input signal. This inability is indicated by the relatively low non-linear enhancement achieved for these larger systems as well as the inability to ratio shape on the largest tPUK systems. The time window limit of the pulse shaper is a result of spatio-temporal coupling, as discussed in 3.1.4. However, spatio-temporal coupling introduces more experimental complications. Spatio-temporal coupling effects cause the pulse shaper output to distort spatially [23, 46, 47]. This distortion decreases input coupling to the chip significantly. The distortion is also not constant. As different phases are programmed on the pulse shaper the spatial distortion of the shaper output changes. Because of fluctuations in the spatial distortion, the input coupling efficiency will also fluctuate. Although a linear

detector is included in the non-linear detection setup to compensate for these fluctuations, they still cause a significant amount of noise in the non-linear output signal.

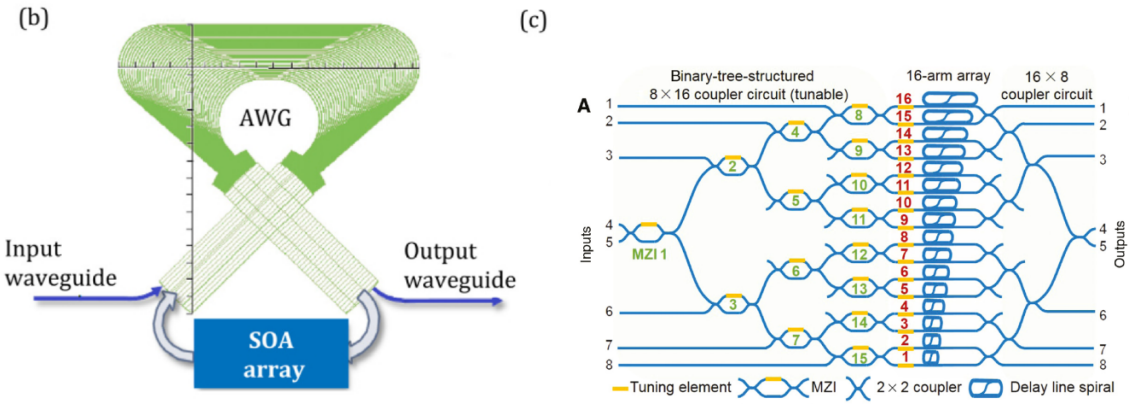

Figure 6.1: *Left*: A pulse shaper design based on the use of arbitrary waveguide gratings (AWGs). Adapted from [48]. *Right*: A pulse shaper design consisting of a network of delay lines. Adapted from [49].

4f pulse shapers are especially prone to spatio-temporal coupling effects [23]. Therefore it could be wise to switch to another pulse shaper design that suffers less from spatio-temporal coupling. An integrated pulse shaper could be a promising alternative to replace our current 4f setup. Such a device is also more suited for real world-applications for the same reasons as integrated tPUKs are. Integrated pulse shapers have already been presented in other literature. These include designs based on arrayed waveguide gratings and networks of delay lines [48–50]. See figure 6.1 for illustrations of such designs. These designs have no problem surpassing the resolution of the current pulse shaper but their maximum time window may be limited.

Another option is setting up a fiber-based pulse shaper. In such a system an optical pulse is first stretched in time. It is then modulated into a desired time structure. Finally, it is again compressed back to its original duration [51]. By first stretching the pulse in time one can modulate the pulse with much greater temporal resolution. This modulation would have to be performed by a device such as an arbitrary waveform generator. Further practical details about such a technique still have to be worked out.

6.3 Non-linear detection

There are still a lot of improvements to be made to the non-linear detection setup. The current setup consists of one non-linear photodiode that can measure one output at a time. Shaping efforts that focus on improving the ratio between the non-linear intensity measured at both outputs require feedback from both outputs. The solution employed currently is to switch the output coupling lens between the two outputs for every shaping iteration. This means that both outputs are not measured at the same time. The output signals are rather noisy due to the earlier mentioned fluctuations in input coupling efficiency. Taking the ratio of two noisy signals measured at different times introduces yet more noise to the feedback signal. Introducing a second detector and amplifier would allow us to measure both output signals at the same time and eliminate this particular problem. Ratio shaping can then also be performed twice as fast, as no switching of the output lens is required anymore.

Another experimental practicality is the detection efficiency and the fact that the non-linear detector still features a small linear absorption. These limitations become especially apparent for the larger tPUK systems, where the output intensity is rater low (< 0.5 mW). This limits the maximum non-linear enhancement that can be achieved. To eliminate or at least reduce the linear absorption problem, other methods of non-linear detection can be tried. A possible method would be to use a non-linear crystal for frequency doubling. As frequency doubling is a second-order non-linear process it scales with the square of the input intensity, similar to 2-photon absorption. The non-linear crystal would take the chip output centered around 800 nm and produce a 400 nm output with a certain efficiency. Any remaining 800 nm light can then be filtered out using some low-pass filters. Linear detection can then be used to measure the 400 nm signal.
Practical efforts have already been undertaken into this alternative detection method. So far, this alternative method has not yielded better non-linear detection efficiencies than the current 2-photon absorption method. Unfortunately, silicon photodiodes have a very low detection efficiency at 400 nm. It is not unlikely that the setup may be altered to work with a laser source producing pulses around 1550 nm in the future. Frequency doubling then produces 775 nm light which can be efficiently detected using silicon photodiodes. Thus making non-linear detection methods using frequency doubling very suitable in that eventuality.

Apart from the already mentioned detection improvements, there are many more possible alternatives. An alternative option may be to make use of a lock-in detection method. By using such a method, one can eliminate a large amount of 1/f noise from the non-linear signal, thus improving the signal-to-noise ratio. Another possibility is to make use of gated-detection methods. In such a technique, we can let the output of a tPUK sample interfere with a reference pulse on a non-linear crystal. With other interference parameters correctly set, the maximum non-linear output generated in a process like second harmonic generation is determined by the likeness of the two pulse time structures. We retrieve the maximum non-linear signal if the time structure of the tPUK output is the same as the reference pulse. As a reference pulse, the original laser output can be used. The non-linear output signal will then be largest if the temporal scrambling of the tPUK is undone by the pulse shaper and the output pulse again has its original time structure. An important benefit of gated-detection methods is the fact that one can choose the reference output to be rather large. This way the non-linear crystal is operating in an intensity range where it is efficient, regardless of the amplitude of the tPUK output.

7. Conclusion and outlook

Using a Michelson interferometer, we have experimentally characterized integrated tPUK systems, consisting of networks of ring resonators, for three distinct system sizes. We have shown that the systems possess transmission characteristics similar to those that were predicted with a theoretical model. By comparing the transmission of identically designed tPUK systems, fabricated on the same chip, it was shown that manufacturing errors ensure unclonability of the tPUK systems. Also shown is that the directional couplers present in the tPUK systems were fabricated with a lower intensity coupling ratio than originally designed.

To improve on the current tPUK design, a new unit cell design has been put forward. The theoretical model covering the current design was expanded to be able to describe this new design and predictions of its transmission characteristics were made. The new design can be used to produce smaller systems that still show tPUK-like transmission characteristics, effectively reducing transmission losses.

Temporal wavefront shaping has been performed on the input of the tPUK samples. Shaping efforts have shown that it is possible to increase the non-linear signal at a system output of choice for all systems sizes. Additionally, we have demonstrated that temporal wavefront shaping can skew the non-linear intensity ratio between the outputs of an integrated tPUK system towards an output of choice. This has been demonstrated for a tPUK system consisting of 13 unit cells, where shaping efforts achieved an output non-linear intensity ratio of factor 3. Although this has not been achieved for a 46 cell system as of yet, suggestions have been put forward to improve experimental conditions. These are thought to make ratio shaping possible for the 46 cell system.

7.1 Outlook

Work is being continued on the integrated tPUK project. In cooperation with LioniX, new photonic chips will be fabricated. These new chips may include an integrated pulse shaper, based on an AWG design or delay line networks. This integrated pulse shaper would replace the current 4f pulse shaper setup. Alternatively, there are also some non-integrated options for a new pulse shaper. Furthermore, new integrated tPUK chips may be fabricated. These could include the new unit cell design presented in this thesis to allow for lower transmission losses. They will most likely also include further design improvements that allow for easier characterization of the tPUK chips. Features such as a single straight waveguide might allow for the integrated tPUKs to be studied using a phase-sensitive Mach-Zehnder interferometer.

Another likely future possibility is adapting the setup to work with a 1550 nm pulsed laser source. This is a wavelength range commonly used in telecommunication applications. Studying integrated tPUK's in this wavelength range will thus more closely resemble their eventual application conditions. This wavelength range also provides new opportunities for an improved non-linear detection setup. tPUK functionality in the few photon regime, as required for tPEAC, may then also be investigated.

8. Acknowledgements

Let me start by thanking my supervisor Pepijn Pinkse for all the help, advice, and direction he provided to me and the project. I always enjoyed our discussions and I was very happy with the new interesting research ideas that flowed from them. Next, let me also thank Matthijs Velsink. Starting out the project in the lab with you helped me to quickly get familiar with the experimental setup. As they say: "Een goed begin is het halve werk". Also when you left for your new position at ARCNL, you were still available for discussions, which were not only valuable to the project but also a lot of fun. I would also like to thank Daan Stellinga. Thank you for all the help you provided in the final stages of this thesis. I really like the ideas you have in mind for the next stages of the project and look forward to helping you get things started in that direction. Thanks also goes out to Hans Kanger, for being the external member of the graduation committee.

I would like to thank all the members of AQO. Chris, Reinier, Frank, and Malaquias, I was very happy that I was allowed to be at the university in person during the ongoing pandemic and work, discuss, and joke around with you guys. Chris, I promise to finally come drink those specialty beers with you now that this thesis is finished. Let me also thank Bert from LPNO for lending me some devices during the project.

A big thanks also goes to my friends and family, who all have provided me with so much support over the past years. Especially during the pandemic this past year, where I think we all needed some more support from each other. And last but not least, Kirsten, thank you so much for being there with me over the past years. We've kept each other sane this past year and I know we will continue to do so in the future. As you always say: "Our love is like the stars".

A. Appendix

A.1 Phase shift method

In optics, the "phase shift" method can be used to determine the relative phase difference between frequencies after having traveled through a device under testing (DUT) [52, 53]. Here a short introduction to the method and also its limitations are given.

The phase shift method makes use of a monochromatic optical source that is amplitude modulated using an RF signal. This modulated signal is then sent through the DUT after which it is detected using a photo-diode. See figure A.1 for a simple schematic representation of the "phase shift" method.

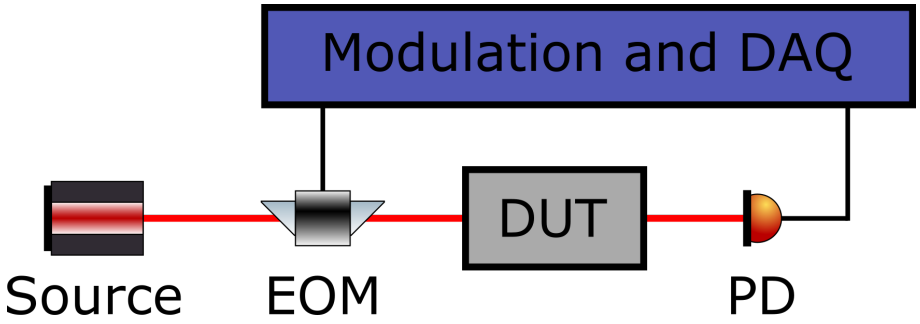

Figure A.1: A schematic representation of a simple "phase shift" setup. An EOM is used to modulate the amplitude of a monochromatic source. The output signal is detected using a photo-diode.

Modulating the source, of frequency ω_S ,with a sinusoidal RF signal, of frequency ω_M, results in a field, $E_{in}(t)$, consisting of two frequency components at $\omega_S + \omega_M$ and $\omega_S - \omega_M$. See eq (A.1) for an expression of $E_{in}(t)$ and $E_{in}(\omega)$.

$$\begin{aligned} E_{in}(t) &= e^{i\omega_S t}\sin(\omega_M t) = \frac{1}{2i}[e^{i(\omega_S+\omega_M)t} - e^{i(\omega_S-\omega_M)t}] \\ \rightarrow E_{in}(\omega) &= \frac{1}{2i}[\delta(\omega-(\omega_S+\omega_M)) - \delta(\omega-(\omega_S-\omega_M))] \end{aligned} \tag{A.1}$$

The DUT will perform a transformation, $T(\omega)$, on the input's amplitude and phase. Eq. A.2 shows how this transformation is applied.

$$E_{out}(\omega) = E_{in}(\omega)T(\omega) \tag{A.2}$$

$T(\omega)$ can be written in it general form: $A_\omega e^{i\phi_\omega}$. Using this, the general form of the outgoing field as a function of time can also be determined by performing an inverse Fourier transform, see eq. (A.3).

$$\begin{aligned} E_{out}(t) &= \frac{1}{2\pi}\int E_{out}(\omega)e^{i\omega t}dt \\ &= \frac{1}{4\pi i}[A_{\omega_+}e^{i(\omega_+)t+i\phi_{\omega_+}} - A_{\omega_-}e^{i(\omega_-)t+i\phi_{\omega_-}}] \end{aligned} \tag{A.3}$$

Where $\omega_+ = \omega_S + \omega_M$ and $\omega_+ = \omega_S - \omega_M$
Having determined the outgoing field as a function of time, one can then derive the outgoing intensity that will be measured using a photo-diode. This is done in eq. (A.4).

$$\begin{aligned} I_{out}(t) &= |E_{out}(t)|^2 \\ &= \frac{1}{16\pi^2}[A_{\omega_+}^2 + A_{\omega_-}^2 - A_{\omega_+}A_{\omega_-}(e^{i(2\omega_M t+(\phi_{\omega_+}-\phi_{\omega_-}))} + e^{-i(2\omega_M t+(\phi_{\omega_+}-\phi_{\omega_-}))})] \\ &= \frac{1}{16\pi^2}[A_{\omega_+}^2 + A_{\omega_-}^2 - 2A_{\omega_+}A_{\omega_-}\cos(2\omega_M t + (\phi_{\omega_+} - \phi_{\omega_-}))] \\ &= \frac{1}{16\pi^2}[A_{\omega_+}^2 + A_{\omega_-}^2 - 2A_{\omega_+}A_{\omega_-}] + \frac{A_{\omega_+}A_{\omega_-}}{4\pi^2}\sin^2\left(\omega_M t + \frac{\phi_{\omega_+} - \phi_{\omega_-}}{2}\right) \end{aligned} \tag{A.4}$$

From eq. (A.4) it becomes clear that the AC term in the measured intensity is proportional to $\sin^2\left(\omega_M t + \frac{\phi_{\omega_+}-\phi_{\omega_-}}{2}\right)$. After removing the DC data the AC term can then be compared to the RF signal used in the initial modulation to retrieve the phase: $\frac{1}{2}(\phi_{\omega_+} - \phi_{\omega_-})$.
From this mathematical examination of the "phase shift" method it should be clear how the phase difference between two frequencies acquired when propagating through the DUT, $(\phi_{\omega_+} - \phi_{\omega_-})$, is obtained. By scanning the frequency of the monochromatic source over a certain frequency range it is possible to construct a spectrum of relative phases. To construct this spectrum a frequency is chosen to be the starting point. This frequency is defined as the zero phase mark. Then one constructs the rest of the spectrum by stitching together the measured phase differences. This process is illustrated in figure A.2.

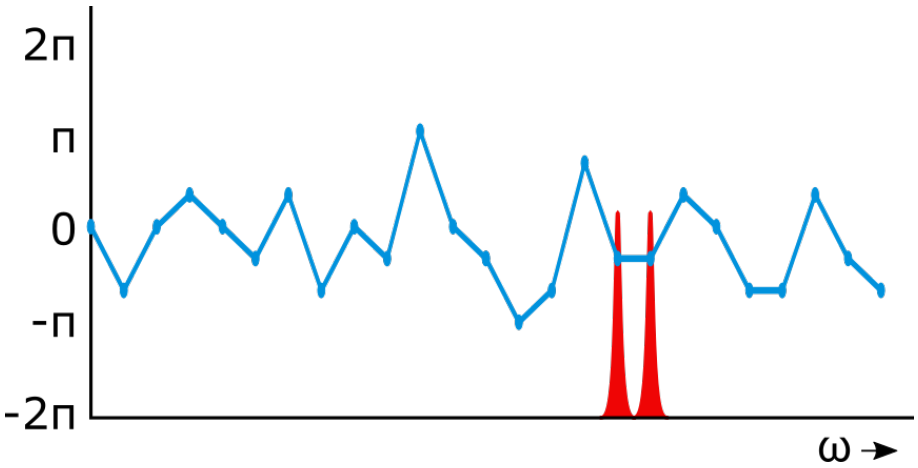

Figure A.2: This figure illustrates how a phase spectrum can be constructed. The measured phase differences are stitched together to form a complete spectrum. When constructing the spectrum the modulation side bands, depicted in red, are scanned through a specified frequency range.

Practical considerations, requirements and limits

Having briefly explained the workings of the "phase shift" method it is now interesting to elaborate on the practical considerations when applying this method. What determines the resolution in phase and in frequency? What experimental requirements are noteworthy? Are there certain DUT's unsuitable for this method?

A.1.1 Resolution

The frequency resolution for the "phase shift" method is determined by the modulation frequency used and also by the accuracy in tuning the carrier frequency. Available to us is a wavemeter that can determine the carrier frequency with an accuracy of about ± 0.05 pm ($\approx \pm$ 25 MHz @ 800 nm). Using a modulation frequency of 50 MHz would then result in us having a frequency resolution of approximately 100 $\pm$ 25 MHz. Multiple measurements are performed at every frequency step to provide enough data for fitting a sine fit. Increasing the number of measurements taken will improve the quality of the fit and thus the accuracy of the determined phase.

A.1.2 Experimental requirements

In general, the "phase shift" method is not especially demanding experimentally. The main requirements are the EOM and the RF modulator. Apart from that photo-diodes with sampling range in the same order as the modulation frequency are required. With typical modulation frequencies of 100 MHz these photo-diode requirements are not very strict.

A.1.3 Limitations

There are some limitations to the "phase shift" method. The main limitation is the fact that the method can only determine the relative phase between frequencies. It cannot determine the absolute phase acquired by a certain frequency.
As a consequence, the "phase shift" method is not suitable for determining the phase difference between a sample's different spatial outputs. Take for example a photonic chip featuring multiple waveguide outputs of different optical path lengths. Comparing the phase difference between the sidebands at different outputs is of no use as the sidebands acquire the same phase when traveling through a longer waveguide, neglecting effects such as dispersion, etc.

Bibliography

[1] F. Cohen, *A short history of Cryptography.* 1990, (accessed 2021-05-06). [Online]. Available: `http://all.net/edu/curr/ip/Chap2-1.html`.

[2] D. J. Bernstein, N. Heninger, P. Lou, *et al.*, "Post-quantum RSA," in *Post-Quantum Cryptography*, ser. Lecture Notes in Computer Science, Springer International Publishing, 2017.

[3] J. Proos and C. Zalka, "Shor's discrete logarithm quantum algorithm for elliptic curves," *arXiv preprint quant-ph/0301141*, 2003.

[4] P. W. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," in *Proceedings 35th Annual Symposium on Foundations of Computer Science*, 1994.

[5] J. Daemen and V. Rijmen, "Aes proposal: Rijndael," 1999.

[6] L. K. Grover, "A fast quantum mechanical algorithm for database search," in *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, 1996.

[7] C. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, 1984.

[8] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, *et al.*, "The security of practical quantum key distribution," *Rev. Mod. Phys.*, vol. 81, no. 3, 2009.

[9] S. A. Goorden, M. Horstmann, A. P. Mosk, *et al.*, "Quantum-secure authentication of a physical unclonable key," *Optica*, vol. 1, no. 6, 2014.

[10] M. Velsink, *Time-domain wavefront shaping for secure communication*, 2019.

[11] R. Uppu, T. A. W. Wolterink, S. A. Goorden, *et al.*, "Asymmetric Cryptography with Physical Unclonable Keys," *arXiv:1802.07573*, 2018.

[12] D. Marcuse and C. Lin, "Low dispersion single-mode fiber transmission - the question of practical versus theoretical maximum transmission bandwidth," *IEEE Journal of Quantum Electronics*, vol. 17, no. 6, 1981.

[13] R. Pappu, B. Recht, J. Taylor, *et al.*, "Physical One-Way Functions," *Science*, vol. 297, no. 5589, 2002.

[14] I. N. Papadopoulos, S. Farahi, C. Moser, *et al.*, "Focusing and scanning light through a multimode optical fiber using digital phase conjugation," *Opt. Express*, vol. 20, no. 10, 2012.

[15] F. van Beijnum, E. G. van Putten, A. Lagendijk, *et al.*, "Frequency bandwidth of light focused through turbid media," *Opt. Lett.*, vol. 36, no. 3, 2011.

[16] N. C. Bruce, F. E. W. Schmidt, J. C. Dainty, *et al.*, "Investigation of the temporal spread of an ultrashort light pulse on transmission through a highly scattering medium," *Appl. Opt.*, vol. 34, no. 25, 1995.

[17] A. Tajalli, D. J. McCabe, D. R. Austin, *et al.*, "Characterization of the femtosecond speckle field of a multiply scattering medium via spatio-spectral interferometry," *J. Opt. Soc. Am. B*, vol. 29, no. 6, 2012.

[18] M. A. Webster, K. J. Webb, A. M. Weiner, *et al.*, "Temporal response of a random medium from speckle intensity frequency correlations," *J. Opt. Soc. Am. A*, vol. 20, no. 11, 2003.

[19] S. M. Popoff, G. Lerosey, M. Fink, *et al.*, "Controlling light through optical disordered media: Transmission matrix approach," *New J. Phys.*, vol. 13, no. 12, 2011.

[20] I. M. Vellekoop and A. P. Mosk, "Focusing coherent light through opaque strongly scattering media," *Opt. Lett.*, vol. 32, no. 16, 2007.

[21] W. Bogaerts, S. K. Selvaraja, P. Dumon, *et al.*, "Silicon-on-Insulator Spectral Filters Fabricated With CMOS Technology," *IEEE J. Sel. Top. Quantum Electron.*, vol. 16, no. 1, 2010.

[22] S. J. Mason, "Feedback theory: Further properties of signal flow graphs," 1956.

[23] A. Monmayrant, S. Weber, and B. Chatel, "A newcomer's guide to ultrashort pulse shaping and characterization," *J. Phys. B At. Mol. Opt. Phys.*, vol. 43, no. 10, 2010.

[24] B. Škorić, P. W. H. Pinkse, and A. P. Mosk, "Authenticated communication from quantum readout of PUFs," *Quantum Inf. Process.*, vol. 16, no. 8, 2017.

[25] D. Bruss, A. Ekert, and C. Macchiavello, "Optimal universal quantum cloning and state estimation," *Physical Review Letters*, vol. 81, no. 12, 1998.

[26] "Tsunami User's Manual," Spectra Physics, Tech. Rep., 2002.

[27] J.-C. M. Diels, J. J. Fontaine, I. C. McMichael, *et al.*, "Control and measurement of ultrashort pulse shapes (in amplitude and phase) with femtosecond accuracy," *Appl. Opt.*, vol. 24, no. 9, 1985.

[28] J.-C. Diels and W. Rudolph, *Ultrashort Laser Pulse Phenomena*. Elsevier, 2006.

[29] C. G. H. Roeloffzen, M. Hoekman, E. J. Klein, *et al.*, "Low-Loss Si3N4 TriPleX Optical Waveguides: Technology and Applications Overview," *IEEE J. Sel. Top. Quantum Electron.*, vol. 24, no. 4, 2018.

[30] A. Monmayrant and B. Chatel, "New phase and amplitude high resolution pulse shaper," *Rev. Sci. Instrum.*, vol. 75, no. 8, 2004.

[31] "Spatial Light Modulator User's Manual Rev. 1.5," Cambridge Research & Instrumentation, Tech. Rep.

[32] C. Palmer, *Diffraction Grating Handbook*. Rochester, New York: Richardson Gratings, Newport Corporation, 2014.

[33] A. M. Weiner, "Femtosecond pulse shaping using spatial light modulators," *Rev. Sci. Instrum.*, vol. 71, no. 5, 2000.

[34] I. M. Vellekoop, "Feedback-based wavefront shaping," *Opt. Express*, vol. 23, no. 9, 2015.

[35] B. Döpke, J. C. Balzer, and M. R. Hofmann, "Phase and amplitude calibration of dual-mask spatial light modulator for high-resolution femtosecond pulse shaping," *Electron. Lett.*, vol. 51, no. 8, 2015.

[36] S.-I. Shin and Y.-S. Lim, "Simple Autocorrelation Measurement by Using a GaP Photoconductive Detector," *J. Opt. Soc. Korea*, vol. 20, no. 3, 2016.

[37] E. Z. Chong, T. F. Watson, and F. Festy, "Autocorrelation measurement of femtosecond laser pulses based on two-photon absorption in GaP photodiode," *Appl. Phys. Lett.*, vol. 105, no. 6, 2014.

[38] D. T. Reid, M. Padgett, C. McGowan, *et al.*, "Light-emitting diodes as measurement devices for femtosecond laser pulses," *Opt. Lett.*, vol. 22, no. 4, 1997.

[39] B. Redding and H. Cao, "Using a multimode fiber as a high-resolution, low-loss spectrometer," *Opt. Lett.*, vol. 37, no. 16, 2012.

[40] B. Redding, S. M. Popoff, and H. Cao, "All-fiber spectrometer based on speckle pattern reconstruction," *Opt. Express*, vol. 21, no. 5, 2013.

[41] D. Loterie, D. Psaltis, and C. Moser, "Bend translation in multimode fiber imaging," *Opt. Express*, vol. 25, no. 6, 2017.

[42] W. Xiong, P. Ambichl, Y. Bromberg, *et al.*, "Principal modes in multimode fibers: Exploring the crossover from weak to strong mode coupling," *Opt. Express*, vol. 25, no. 3, 2017.

[43] I. SPSS, *Pearson correlations – quick introduction*, `https://www.spss-tutorials.com/pearson-correlation-coefficient`, (accessed 2021-05-06), 2021.

[44] I. M. Vellekoop and A. P. Mosk, "Phase control algorithms for focusing light through turbid media," *Opt. Commun.*, vol. 281, no. 11, 2008.

[45] D. B. Conkey, A. N. Brown, A. M. Caravaca-Aguirre, *et al.*, "Genetic algorithm optimization for focusing through turbid media in noisy environments," *Opt. Express*, vol. 20, no. 5, 2012.

[46] F. Frei, A. Galler, and T. Feurer, "Space-time coupling in femtosecond pulse shaping and its effects on coherent control," *The Journal of chemical physics*, vol. 130, no. 3, 2009.

[47] M. M. Wefers and K. A. Nelson, "Space-time profiles of shaped ultrafast optical waveforms," *IEEE Journal of Quantum Electronics*, vol. 32, no. 1, 1996.

[48] A. J. Metcalf, H.-J. Kim, D. E. Leaird, *et al.*, "Integrated line-by-line optical pulse shaper for high-fidelity and rapidly reconfigurable rf-filtering," *Optics Express*, vol. 24, no. 21, 2016.

[49] Y. Xie, L. Zhuang, and A. J. Lowery, "Picosecond optical pulse processing using a terahertz-bandwidth reconfigurable photonic integrated circuit," *Nanophotonics*, vol. 7, no. 5, 2018.

[50] N. K. Fontaine, R. P. Scott, C. Yang, *et al.*, "Compact 10 ghz loopback arrayed-waveguide grating for high-fidelity optical arbitrary waveform generation," *Optics letters*, vol. 33, no. 15, 2008.

[51] B. T. Bosworth and M. A. Foster, "High-speed ultrawideband photonically enabled compressed sensing of sparse radio frequency signals," *Optics letters*, vol. 38, no. 22, 2013.

[52] L. Zhuang, D. Marpaung, M. Burla, *et al.*, "Low-loss, high-index-contrast si 3 n 4/sio 2 optical waveguides for optical delay lines in microwave photonics signal processing," *Optics express*, vol. 19, no. 23, 2011.

[53] C. Roeloffzen, L. Zhuang, R. Heideman, *et al.*, "Ring resonator-based tunable optical delay line in lpcvd waveguide technology," in *Proc. 9th IEEE/LEOS Symp. Benelux*, 2005.