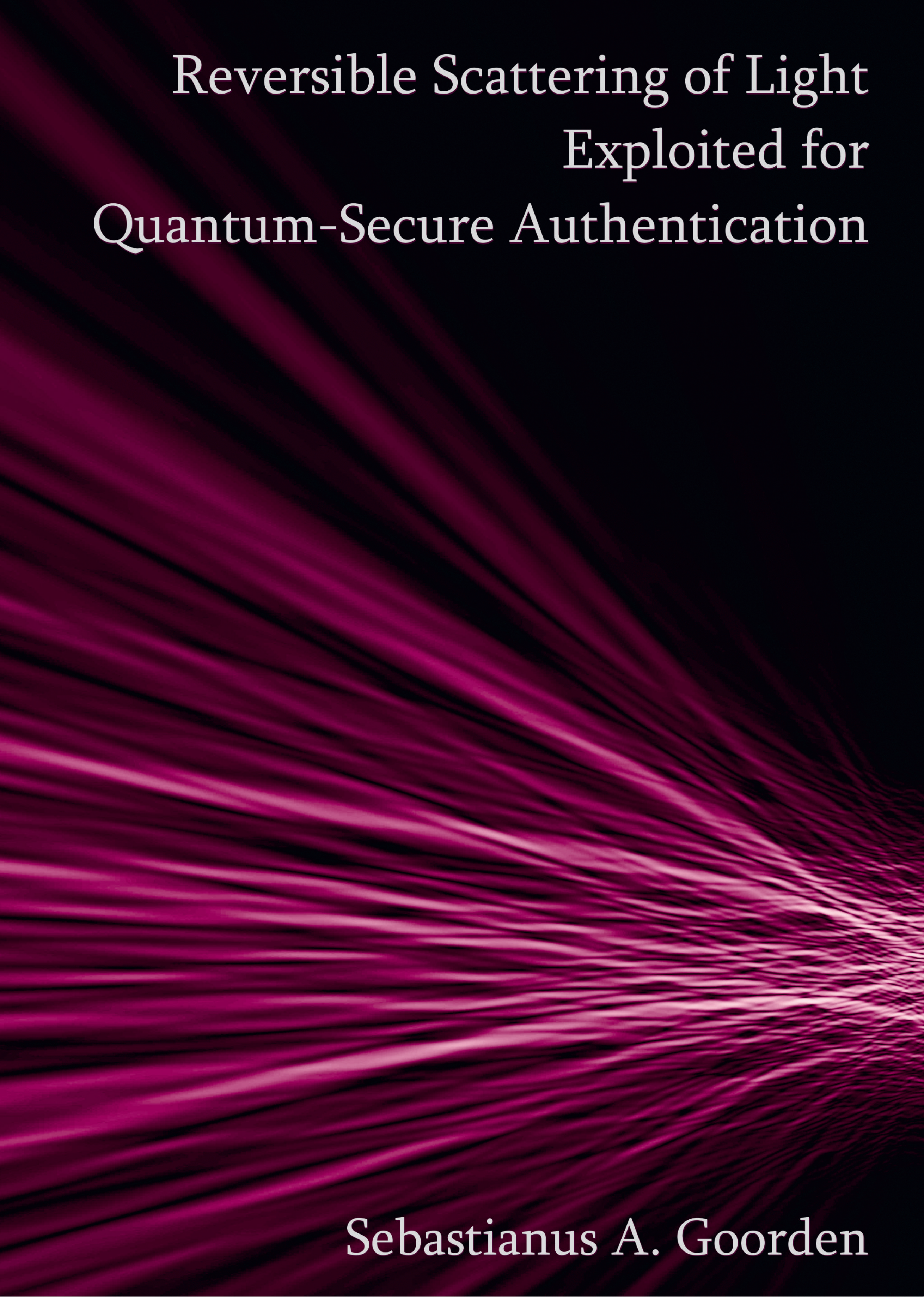
Reversible Scattering of Light Exploited for Quantum-Secure Authentication



Sebastianus A. Goorden

Reversible scattering of light exploited for quantum-secure authentication

Omkeerbare verstrooiing van licht benut voor quantum-veilige authenticatie

Promotiecommissie

Promotoren	prof. dr. A.P. Mosk prof. dr. P.W.H. Pinkse
Overige leden	prof. dr. C. Fallnich prof. dr. S. Gigan dr. B. Škorić prof. dr. B.M. Terhal prof. dr. R.N.J. Veldhuis

The work described in this thesis is financially supported by the stichting FOM which is financially supported by the 'Nederlandse Organisatie voor Wetenschappelijk Onderzoek' (NWO). Additional funding is provided by ERC and MESA+.

It was carried out at the
Complex Photonic Systems Group,
Department of Science and Technology
and MESA+ Institute for Nanotechnology,
University of Twente, P.O. Box 217,
7500 AE Enschede, The Netherlands.

REVERSIBLE SCATTERING OF LIGHT EXPLOITED FOR QUANTUM-SECURE AUTHENTICATION

PROEFSCHRIFT

ter verkrijging van
de graad van doctor aan de Universiteit Twente,
op gezag van de rector magnificus,
prof. dr. H. Brinksma,
volgens besluit van het College voor Promoties
in het openbaar te verdedigen
op vrijdag 10 juli 2015 om 14.45 uur

door

Sebastianus Adrianus Goorden

geboren op 19 september 1987
te Roosendaal en Nispen, Nederland

Dit proefschrift is goedgekeurd door:

prof. dr. A.P. Mosk en prof. dr. P.W.H. Pinkse

Voor mijn ouders

Contents

CHAPTER 1
Introduction

1.1 Coherent light scattering

A light wave that interacts with matter induces dipole moments in the atoms or molecules that make up the material. These induced oscillating dipoles coherently radiate a fraction of the incident light into dipole waves. The macroscopic optical response of a material strongly depends on the microscopic distribution of dipoles. In transparent media, such as air, water and glass, dipoles are distributed more or less uniformly and densely at the micrometer scale of the optical wavelength. As a result the radiated dipole waves interfere to slow down the propagating wavefront, a process known as refraction. In media such as boiled egg, fog, milk, white paint and skin, dipoles are inhomogeneously distributed. In this case the radiated waves interfere randomly and light is scattered. The scattered light is the sum of all scattered and multiple-scattered waves and is intractible for randomly positioned clusters of dipoles [1]. Light entering such media is completely scrambled and appears to diffuse in all directions, making it impossible to look through them. Until recently, multiple-scattering of light was considered an impediment to applications including optical imaging, optical communication and collection of solar energy.

The work described in this thesis focuses on understanding, controlling and exploiting the propagation of light in multiple-scattering media. Phenomena such as "open channels" and "long-lived modes" are investigated. These phenomena allow extraordinarily high transmission and extraordinarily long traversal times of light through multiple-scattering media. The complexity of scattered waves is a challenge in many applications, but may itself also be exploited. We converge towards using multiple-scattering media for secure authentication of objects. The work in this thesis is based on exciting recent developments regarding control over light in scattering media, which are summarized in Section 1.2. Due to these results it is becoming ever more apparent that multiple-scattering can be harnessed and may be exploited for a broad range of applications, as we describe in Section 1.3. An outline of the rest of this thesis is provided in Section 1.4.

1.2 Control over multiple light scattering

At first sight, light in a multiple-scattering medium is much like a ball in a pinball machine: it bounces around more or less randomly and apparently uncontrollably.

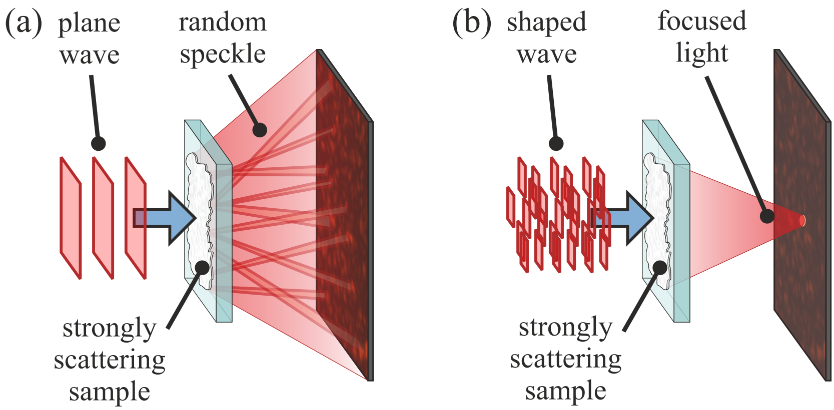


Figure 1.1: (a) An uncontrolled light beam passing through a multiple-scattering medium forms a random speckle pattern. (b) Shaping the light beam allows the light to focus behind the multiple-scattering medium. Image from [2].

This view was changed dramatically by the invention of wavefront shaping by the COPS group in 2007 [2], after predictions by Freund [3]. In terms of the pinball metaphor they manipulated the ball so that it hits the jackpot every time.

Wavefront shaping of light through a multiple-scattering medium is illustrated in Fig. 1.1. Coherent light transmitted through a multiple-scattering medium typically forms a random pattern called speckle, as is shown in Fig. 1.1(a). However, by shaping the incident light appropriately, one can choose where the light goes after passing through the scattering layer. In Fig. 1.1(b), the light is focused in one point.

The recent development of spatial light modulators is vital for controlling light in multiple-scattering media. Spatial light modulators (SLMs) are computer-controlled devices that allow control over the amplitude, phase and/or polarization of light at a high spatial resolution. The majority of the experiments, including the initial ones, that control light in multiple-scattering media use liquid crystal-based SLMs [4]. Digital micromirror-based SLMs [5] are, however, rapidly gaining ground. These micromirror devices have a very high speed, of which the benefit is especially clear when feedback-based control algorithms are used.

A feedback mechanism is at the basis of the wavefront shaping experiments performed at COPS. The phase imprinted on the wavefront by groups of SLM pixels is changed sequentially and each group of pixels is set to maximize the intensity in the desired focus spot. Such algorithms [6] were used to achieve many exciting results [7]. Wavefront shaping was used to demonstrate the existence of open channels in multiple-scattering media [8] and enhance or decrease the total transmission [9], proving theoretical predictions from long before [10–13]. It enables focusing inside a scattering medium [14] and the use of a multiple-scattering medium as a spectral filter [15, 16], tunable wave plate [17, 18] or tunable beamsplitter [19]. It makes it possible to use a scattering medium as a lens [20] that allows record-high resolution in linear optical microscopy [21]. Spatial control over light pulses in a multiple-scattering medium allows focusing of light at selected points in time [22–24]. Moreover, such experiments can be performed at very high speeds in the order of 10 ms [25].

In transmission matrix measurements the experiment is parallelized to obtain additional information, as was first demonstrated by Popoff and co-workers [26]. This enables imaging through multiple-scattering media without requirement of an angular memory effect for scanning the focus. Knowledge of the transmission matrix allows efficient coupling to open channels [27]. Transmission matrix measurements are also used to image through multimode fibers, where the fiber is treated as a random scattering medium [28].

Phase conjugation is the single-shot equivalent to feedback-based wavefront shaping. In phase conjugation, a source is placed at the desired focus point and the scattered light field is measured. Phase conjugation of the measured field reproduces a focus. Analog phase conjugation through a multiple-scattering medium [29], using a photorefractive material, as well as digital optical phase conjugation [30, 31], which uses an SLM, were demonstrated in recent years. Iterative phase conjugation was used to demonstrate enhanced energy transmission through a scattering medium [32]. Phase conjugation is combined with photoacoustic tagging of photons to form a highly versatile tool for focusing and imaging inside multiple-scattering media [33–35].

Wave control through scattering media has also been demonstrated with other waves and in other regimes. For example, ultrasound waves and microwaves have been focused through multiple-scattering media [36–40]. Water waves have been focused as well [41]. Microwaves are used to investigate channels and modes of multiple-scattering media [42–44]. The propagation of light through weakly or single scattering media such as the atmosphere and ground glass diffusers is controlled in adaptive optics [45], where phase conjugation [46] as well as feedback methods [47] are used.

1.3 Applications of control over multiple light scattering

Control over light in multiple-scattering media is expected to be useful in a broad range of areas. We discuss applications in healthcare, sensing, microscopy, solar energy, lighting and security.

Healthcare is an important driver of research into controlling light in multiple-scattering media. Biological tissue is a multiple-scattering medium. Control over light propagation in the body allows new imaging methods such as [34, 35], but also could be used to enhance existing imaging methods. Methods such as optical coherence tomography and photo-acoustic tomography [48] can only image up to the depth to which light diffuses into the body. By shaping the light to penetrate deeper into the body, the imaging depth of these methods can be enhanced [49]. Another application of guiding light inside the body is found in optogenetics [50].

This is a new field in which light stimulates certain types of cells, for example neurons, that are tagged with light-sensitive proteins. This allows control over and investigation of these cells. Delivery of the required amount of light at the required place is crucial and can be enhanced by shaping light.

Sensors, such as in absorption spectroscopy, can be made more sensitive by exploiting multiple-scattering [51]. Multiple light scattering leads to longer path-lengths and enhances the interaction between light and the medium. For example, the overall absorption of a low concentration analyte can be increased in this way.

Microscopes and other optical systems typically require high-quality optics, of which the complexity and cost increase dramatically with the desired performance. Using a scattering medium as a high-resolution lens may be a sensible alternative [21, 52].

Solar energy has by far the largest potential of all renewable energy sources. A lot of research is done to increase the efficiency of solar cells [53]. Recent research shows that random scattering media can be used to enhance solar cells [54–56]. Shaping of sunlight may enhance the interaction between sunlight and a multiple-scattering solar cell, thereby increasing the absorption efficiency.

Light-emitting diodes (LEDs) are rapidly taking over as the dominant artificial light source, mainly due to their high energy efficiency. Because no efficient green and yellow LEDs exist, white LEDs usually consist of an efficient blue LED in combination with phosphors that convert blue light into a combination of green, yellow and red light in such a way that the result is white light [57]. The phosphors are typically contained in a multiple-scattering medium, which enhances the interaction between blue light and phosphors and mixes the light in color and direction [58]. Shaping the blue light before it enters the multiple-scattering medium may further enhance the interaction between blue light and phosphor, therefore reducing the amount of phosphor needed. Moreover, the light may be shaped to pass through open channels of the scattering layer, reducing the back reflection and therefore increasing the efficiency of the LED.

In security, a multiple-scattering medium is recognized as a valuable asset because of its inherent randomness and unclonability. It can be used to store keys and to authenticate an object in which it is embedded or a person who is holding it [59–61], which may help to prevent cases of e.g. fraud and unauthorized access. Control over light in multiple-scattering media leads to improved security primitives.

1.4 Outline of this thesis

The central theme of this thesis is control over light in multiple-scattering media. Although various applications may benefit from work in this thesis, we converge towards secure authentication of objects.

In Chapter 2 we investigate two fundamental phenomena in multiple-scattering media: open channels and long-lived modes. Open channels allow order unity transmission through disordered media, even if the medium has a low average transmission. Light coupled to long-lived modes of a disordered medium remains inside the medium for a time duration significantly longer than average. Our goal is to improve the understanding of open channels and long-lived modes by finding efficient ways to identify and address them, which may have significant impact on many of the applications described in Section 1.3. The chapter starts by discussing the basic tool for the proposed experiments: digital optical phase conjugation. We then describe a method to identify and address open channels by performing iterative phase conjugation, or ping-pong, with light. Finally, we propose to identify and address long-lived modes by a similar iterative method in which we phase conjugate the first or second frequency derivative of the transmitted field in each iteration. Numerical simulations are performed to predict the effectiveness of these methods and show that efficient coupling of light to open channels and long-lived modes is likely within experimental reach.

In Chapter 3 we address the question of how to obtain accurate control over light. Accurate control over light is what makes it possible to control the propagation of light in multiple-scattering media and is at the basis of most work in this field. We describe a method for controlling light based on a digital micromirror device (DMD), which is an array of aluminum micromirrors that in principle only offer on/off modulation capability. Practically full and independent control over phase and amplitude is obtained by grouping pixels into superpixels. Features of our method such as its precision, speed and resolution are discussed and compared to the state-of-the-art.

In Chapter 4 the apparatus that we built to obtain maximum control over the coupling of light to the modes of photonic structures is described. The apparatus features a frequency-tunable laser as well as vector field synthesizers and detectors on both sides of the sample. It satisfies all experimental requirements for elucidating phenomena such as open channels and long-lived modes and applications such as cryptography with random media.

In Chapter 5 quantum-secure authentication (QSA) of a physical unclonable key is demonstrated. QSA is an object authentication method that uses a multiple-scattering medium as a key. The method requires that a large number of the channels of the key is controlled. The key is authenticated using a number of photons that is lower than the number of controlled channels. We obtain an object authentication method that is secure against copying as well as digital emulation, even if all information about the key is publicly known.

In Chapter 6 we investigate the potential impact of QSA on society and whether there is a market for QSA. We first place QSA into its cryptographic context by comparing it to other object authentication methods. Then, a number of security threats are highlighted and we discuss the potential role of QSA in this context. Specific potential attacks against QSA are also analyzed and we conclude with steps towards valorization of QSA.

Bibliography

[1] P. Sheng, *Introduction to wave scattering, localization and mesoscopic phenomena* (Springer-Verlag Berlin Heidelberg, Germany, 2006). — p.3.

[2] I. M. Vellekoop and A. P. Mosk, *Focusing coherent light through opaque strongly scattering media*, Opt. Lett. **32**, 2309 (2007). — p.4.

[3] I. Freund, *Looking through walls and around corners*, Physica A **168**, 49 (1990). — p.4.

[4] P. Yeh and C. Gu, *Optics of liquid crystal displays* (John Wiley and Sons, Inc., Hoboken, New Jersey, U.S.A., 2010). — p.4.

[5] D. Dudley, W. M. Duncan, and J. Slaughter, *Emerging digital micromirror device (DMD) applications*, Proc. SPIE **4985**, 14 (2003). — p.4.

[6] I. M. Vellekoop and A. P. Mosk, *Phase control algorithms for focusing light through turbid media*, Opt. Commun. **281**, 3071 (2008). — p.4.

[7] A. P. Mosk, A. Lagendijk, G. Lerosey, and M. Fink, *Controlling waves in space and time for imaging and focusing in complex media*, Nature Photon. **6**, 283 (2012). — p.4.

[8] I. M. Vellekoop and A. P. Mosk, *Universal optimal transmission of light through disordered materials*, Phys. Rev. Lett. **101**, 120601 (2008). — p.4.

[9] S. M. Popoff, A. Goetschy, S. F. Liew, A. D. Stone, and H. Cao, *Coherent control of total transmission of light through disordered media*, Phys. Rev. Lett. **112**, 133903 (2014). — p.4.

[10] C. W. J. Beenakker, *Random-matrix theory of quantum transport*, Rev. Mod. Phys. **69**, 731 (1997). — p.4.

[11] O. N. Dorokhov, *Transmission coefficient and the localization length of an electron in N bound disordered chains*, JETP Lett. **36**, 318 (1982). — p.4.

[12] O. N. Dorokhov, *On the coexistence of localized and extended electronic states in the metallic phase*, Solid State Commun. **51**, 381 (1984). — p.4.

[13] P. A. Mello, P. Pereyra, and N. Kumar, *Macroscopic approach to multichannel disordered conductors*, Ann. Phys. **181**, 290 (1988). — p.4.

[14] I. M. Vellekoop, E. G. van Putten, A. Lagendijk, and A. P. Mosk, *Demixing light paths inside disordered metamaterials*, Opt. Express **16**, 67 (2008). — p.4.

[15] J. H. Park, C. Park, H. Yu, and Y. Cho, Y. H. Park, *Active spectral filtering through turbid media*, Opt. Lett. **37**, 3261 (2012). — p.4.

[16] E. Small, O. Katz, Y. F. Guan, and Y. Silberberg, *Spectral control of broadband light through random media by wavefront shaping*, Opt. Lett. **37**, 3429 (2012). — p.4.

[17] J. H. Park, C. Park, H. Yu, Y. H. Cho, and Y. Park, *Dynamic active wave plate using random nanoparticles*, Opt. Express **20**, 17010 (2012). — p.4.

[18] Y. F. Guan, O. Katz, E. Small, J. Y. Zhou, and Y. Silberberg, *Polarization control of multiply scattered light through random media by wavefront shaping*, Opt. Lett. **37**, 4663 (2012). — p.4.

[19] S. R. Huisman, T. J. Huisman, S. A. Goorden, A. P. Mosk, and P. W. H. Pinkse, *Programming balanced optical beam splitters in white paint*, Opt. Express **22**, 8320 (2014). — p.5.

[20] I. M. Vellekoop and C. M. Aegerter, *Scattered light fluorescence microscopy: imaging through turbid layers*, Opt. Lett. **35**, 1245 (2010). — p.5.

[21] E. G. van Putten, D. Akbulut, J. Bertolotti, W. L. Vos, A. Lagendijk, and A. P. Mosk, *Scattering lens resolves sub-100 nm structures with visible light*, Phys. Rev. Lett. **106**, 193905 (2011). — p.5, 6.

[22] J. Aulbach, B. Gjonaj, P. M. Johnson, A. P. Mosk, and A. Lagendijk, *Control of light transmission through opaque scattering media in space and time*, Phys. Rev. Lett. **106**, 103901:1 (2011). — p.5.

[23] O. Katz, E. Small, Y. Bromberg, and Y. Silberberg, *Focusing and compression of ultrashort pulses through scattering media*, Nature Photon. **5**, 372 (2011). — p.5.

[24] D. J. McCabe, A. Tajalli, D. Austin, P. Bondareff, I. A. Walmsley, S. Gigan, and B. Chatel, *Spatio-temporal focusing of an ultrafast pulse through a multiply scattering medium*, Nat. Commun. **2**, 447 (2011). — p.5.

[25] D. B. Conkey, A. M. Caravaca-Aguirre, and R. Piestun, *High-speed scattering medium characterization with application to focusing light through turbid media*, Opt. Express **20**, 1733 (2012). — p.5.

[26] S. M. Popoff, G. Lerosey, R. Carminati, M. Fink, A. C. Boccara, and S. Gigan, *Measuring the transmission matrix in optics: An approach to the study and control of light propagation in disordered media*, Phys. Rev. Lett. **104**, 100601 (2010). — p.5.

[27] M. Kim, Y. Choi, C. Yoon, W. Choi, J. Kim, Q.-H. Park, and W. Choi, *Maximal energy transport through disordered media with the implementation of transmission eigenchannels*, Nature Photon. **6**, 581 (2012). — p.5.

[28] Y. Choi, C. Yoon, M. Kim, T. D. Yang, C. Fang-Yen, R. R. Dasari, K. J. Lee, and W. Choi, *Scanner-free and wide-field endoscopic imaging by using a single multimode optical fiber*, Phys. Rev. Lett. **109**, 203901 (2012). — p.5.

[29] Z. Yaqoob, D. Psaltis, M. S. Feld, and C. Yang, *Optical phase conjugation for turbidity suppression in biological samples*, Nature Photon. **2**, 110 (2008). — p.5.

[30] M. Cui and C. Yang, *Implementation of a digital optical phase conjugation system and its application to study the robustness of turbidity suppression by phase conjugation*, Opt. Express **18**, 3444 (2010). — p.5.

[31] C. L. Hsieh, Y. Pu, R. Grange, and D. Psaltis, *Digital phase conjugation of second harmonic radiation emitted by nanoparticles in turbid media*, Opt. Express **18**, 12283 (2010). — p.5.

[32] X. Hao, L. Martin-Rouault, and M. Cui, *A self-adaptive method for creating high efficiency communication channels through random scattering media*, Sci. Rep. **4**, 5874 (2014). — p.5.

[33] X. Xu, H. Liu, and L. V. Wang, *Time-reversed ultrasonically encoded optical focusing into scattering media*, Nature Photon. **5**, 154 (2011). — p.5.

[34] Y. M. Wang, B. Judkewitz, C. A. DiMarzio, and C. Yang, *Deep-tissue focal fluorescence imaging with digitally time-reversed ultrasound-encoded light*, Nat. Commun. **3**, 928 (2012). — p.5.

[35] K. Si, R. Fiolka, and M. Cui, *Fluorescence imaging beyond the ballistic regime by ultrasound-pulse-guided digital phase conjugation*, Nature Photon.

6, 657 (2012). — p.5.
[36] M. Fink, *Time reversal of ultrasonic fields, Part I: Basic principles.*, IEEE Trans. Ultrason. Ferroelectr. Freq. Control **39**, 555 (1992). — p.5.
[37] M. Fink, *Time reversed acoustics*, Phys. Today **50**, 34 (1997). — p.5.
[38] F. Lemoult, G. Lerosey, J. de Rosny, and M. Fink, *Manipulating spatiotemporal degrees of freedom of waves in random media*, Phys. Rev. Lett. **103**, 173902 (2009). — p.5.
[39] G. Lerosey, J. de Rosny, A. Tourin, A. Derode, G. Montaldo, and M. Fink, *Time reversal of electromagnetic waves*, Phys. Rev. Lett. **92**, 193904 (2004). — p.5.
[40] G. Lerosey, J. de Rosny, A. Tourin, A. Derode, and M. Fink, *Time reversal of wideband microwaves*, Appl. Phys. Lett. **88**, 154101 (2006). — p.5.
[41] A. Przadka, S. Feat, P. Petitjeans, V. Pagneux, A. Maurel, and M. Fink, *Time reversal of water waves*, Phys. Rev. Lett. **109**, 064501 (2012). — p.5.
[42] J. Wang and A. Genack, *Transport through modes in random media*, Nature **471**, 345 (2011). — p.5.
[43] M. Davy, Z. Shi, and A. Z. Genack, *Focusing through random media: Eigenchannel participation number and intensity correlation*, Phys. Rev. B **85**, 035105 (2012). — p.5.
[44] Z. Shi and A. Z. Genack, *Transmission eigenvalues and the bare conductance in the crossover to anderson localization*, Phys. Rev. Lett. **108**, 043901 (2012). — p.5.
[45] R. K. Tyson, *Principles of adaptive optics*, 2nd ed. (Academic Press, New York, U.S.A., 1998). — p.5.
[46] E. N. Leith and J. Upatnieks, *Holographic imagery through diffusing media*, J. Opt. Soc. Am. **56**, 523 (1966). — p.5.
[47] W. B. Bridges, P. T. Brunner, S. P. Lazzara, T. A. Nussmeier, T. R. O'Meara, J. A. Sanguinet, and J. W. P. Brown, *Coherent optical adaptive techniques*, Appl. Opt. **13**, 291 (1974). — p.5.
[48] L. V. Wang and S. Hu, *Photoacoustic tomography: in vivo imaging from organelles to organs*, Science **335**, 1458 (2012). — p.5.
[49] J. Jang, J. Lim, H. Yu, H. Choi, J. Ha, J.-H. Park, W.-Y. Oh, W. Jang, S. Lee, and Y. Park, *Complex wavefront shaping for optimal depth-selective focusing in optical coherence tomography*, Opt. Express **21**, 2890 (2013). — p.5.
[50] O. Yizhar, L. E. Fenno, T. J. Davidson, M. Mogri, and K. Deisseroth, *Optogenetics in neural systems*, Neuron **71**, 9 (2011). — p.5.
[51] V. B. Koman, C. Santschi, and O. J. F. Martin, *Multiscattering-enhanced absorption spectroscopy*, Anal. Chem. **87**, 1536 (2015). — p.6.
[52] H. Yılmaz, E. G. van Putten, J. Bertolotti, A. Lagendijk, W. L. Vos, and A. P. Mosk, *Speckle correlation resolution enhancement of wide-field fluorescence imaging*, arXiv:1410.2079 (2015). — p.6.
[53] A. Polman and H. A. Atwater, *Photonic design principles for ultrahigh-efficiency photovoltaics*, Nature Mater. **11**, 174 (2012). — p.6.
[54] M. Burresi, F. Pratesi, F. Riboli, and D. S. Wiersma, *Complex photonic structures for light harvesting*, Adv. Opt. Mater. (online March 25, 2015).

— p.6.

[55] U. W. Paetzold, M. Smeets, M. Meier, K. Bittkau, T. Merdzhanova, V. Smirnov, D. Michaelis, C. Waechter, R. Carius, and U. Rau, *Disorder improves nanophotonic light trapping in thin-film solar cells*, Appl. Phys. Lett. **104**, 131102 (2014). — p.6.

[56] F. Pratesi, M. Burresi, F. Riboli, K. Vynck, and D. S. Wiersma, *Disordered photonic structures for light harvesting in solar cells*, Opt. Express **21**, A460 (2013). — p.6.

[57] J. Y. Tsao, M. H. Crawford, M. E. Coltrin, A. J. Fischer, D. D. Koleske, G. S. Subramania, G. T. Wang, J. J. Wierer, and R. F. Karlicek Jr., *Toward smart and ultra-efficient solid-state lighting*, Adv. Opt. Mater. **2**, 809 (2014). — p.6.

[58] V. Y. F. Leung, A. Lagendijk, T. W. Tukker, A. P. Mosk, W. L. IJzerman, and W. L. Vos, *Interplay between multiple scattering, emission, and absorption of light in the phosphor of a white light-emitting diode*, Opt. Express **22**, 8190 (2014). — p.6.

[59] R. Pappu, B. Recht, J. Taylor, and N. Gershenfeld, *Physical one-way functions*, Science **297**, 2026 (2002). — p.6.

[60] J. D. R. Buchanan, R. P. Cowburn, A. Jausovec, D. Petit, P. Seem, G. Xiong, D. Atkinson, K. Fenton, D. A. Allwood, and M. T. Bryan, *Forgery: 'fingerprinting' documents and packaging*, Nature **436**, 475 (2005). — p.6.

[61] B. Škorić, *Quantum readout of physical unclonable functions*, Int. J. Quant. Inf. **10**, 1250001 (2012). — p.6.

CHAPTER 2

Investigation of open channels and long-lived modes in disordered media

2.1 Introduction

Wavefront shaping of light through scattering media is a field that is rapidly gaining momentum due to its broad range of applications in e.g. biomedical imaging, defense and security. The growth of the field provides a strong incentive to obtain a more thorough understanding of the properties of scattering media in terms of the optical modes in the spatial and temporal domain. In particular, we focus our attention on two phenomena, "open channels" and "long-lived modes". A light wave with a spatial profile adapted to an open channel has a transmission coefficient of 1 and will pass the scattering layer without back reflection. Open channels exist in scattering layers of arbitrary thickness [1–3], which is highly counterintuitive and may allow, for example, optical imaging and communication through thick media that normally transmit insufficient light. The second phenomenon is a long-lived mode, which is a resonance inside the scattering medium that has a significantly longer lifetime than the average as predicted by diffusion theory. These modes can correspond to diffuse paths or folded paths that are characteristic of resonant cavities [4, 5]. Besides the fundamental interest of understanding the lifetimes of modes in scattering media, finding and addressing long-lived modes may lead to numerous applications. For example, long-lived modes may be useful in biomedical imaging if their corresponding spatial intensity distributions are relatively uniform, and the enhanced light-matter interaction could lead to more accurate sensors and more efficient LEDs and solar cells [6].

In this chapter we describe approaches to investigate and address open channels and long-lived modes in random scattering media using shaped wavefronts. Digital optical phase conjugation, the method we use to shape wavefronts, is described in Section 2.2. In Section 2.3 we discuss the coupling of light to open channels of strongly scattering media. The coupling of light to long-lived modes is described in Section 2.4.

2.2 Optical phase conjugation

Optical phase conjugation is a method typically used for reversing the scattering of light waves. The first experimental demonstration of optical phase conjugation

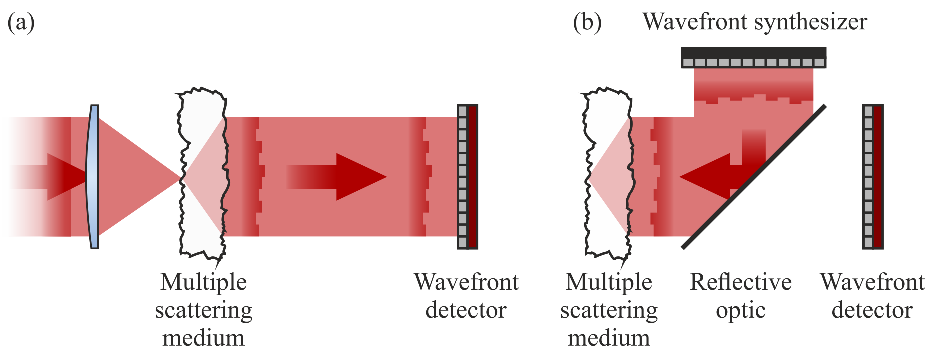


Figure 2.1: Illustration of a phase conjugation procedure. (a) Step 1: recording the wavefront. (b) Step 2: reconstructing the wavefront. Optional (but recommended) collection optics between the scattering medium and the wavefront synthesizer / detector are omitted.

to transmit images through a diffuser used a photographic plate as the phase-conjugate mirror [7]. In the twentieth century, the primary application of optical phase conjugation was in adaptive optics [8], where it is used to improve the quality of images transmitted through weakly scattering media such as the atmosphere. Starting from the 1970s a variety of wavefront correcting devices was developed, including multiple types of segmented mirrors, deformable mirrors and edge-actuated mirrors [8, 9]. These devices typically control $2 - 10^3$ spatial modes, enough to correct for low-order aberrations.

Much more recently it was demonstrated that wavefront shaping can be used to control the propagation of light through strongly multiple-scattering media that completely scramble the light field [10]. This was achieved using spatial light modulators that can control in the order of 10^6 spatial modes and allows e.g. focusing of light through a human tooth or a chicken eggshell, with anticipated applications in areas such as biomedical imaging. Similar results were demonstrated with optical phase conjugation, using photorefractive material [11] or a spatial light modulator [12, 13] to shape the light field.

One can distinguish between digital optical phase conjugation and "analog" nonlinear phase conjugate mirrors [14–16]. Digital optical phase conjugation uses digital devices such as cameras and spatial light modulators for recording and synthesizing wavefronts. Analog optical phase conjugation uses nonlinear effects in e.g. photorefractive materials. Digital optical phase conjugation offers the advantage of a much higher flexibility. Fields can be manipulated at will between the detection and reconstruction phases, making possible e.g. energy gain and phase conjugation of frequency derivatives of transmitted fields. This flexibility is crucial for our purposes, as described in Sections 2.3 and 2.4, and therefore we only consider digital optical phase conjugation from here onward.

The working principle of digital optical phase conjugation is schematically shown in Fig. 2.1. Light is phase conjugated through a multiple-scattering medium. We consider a monochromatic light beam, since multiple-scattering media are highly dispersive. In principle it is possible to conjugate a light beam with arbitrary spatial shape. As an example, we focus the light beam onto the surface of the multiple-scattering medium, after which the light diffuses, as shown in Fig. 2.1(a). A large fraction of the light leaves the sample in the reflection direction (not shown). The rest of the light diffuses through the sample and leaves the sample on the opposite side, forming a speckle pattern propagating through free space. The light propagates towards the wavefront detector, which typically detects the spatially resolved phase and amplitude of a single polarization component of the speckle field. The phase conjugation, illustrated in Fig. 2.1(b), consists in constructing the phase conjugate speckle field using a wavefront synthesizer such as a spatial light modulator. The conjugate speckle field propagates in the backward direction towards the multiple-scattering medium. The light enters the medium and continues to follow the inverted path, ultimately focusing at the position of the original focus.

The fidelity of the phase conjugation process is defined as $F = |E^*_{\text{out}} E_{\text{synth}}|^2$, where E_{out} is the light field in the recording phase and E_{synth} is the synthesized light field, both defined on the sample surface at the side of the phase conjugation apparatus. Both fields are normalized to their total power. A fidelity $F = 1$ means phase conjugation works perfectly[1], whereas $F = 0$ indicates absence of a conjugate field. In order to maximize F one must resolve the vector field E_{out} spatially and synthesize its conjugate, which typically requires high-NA collection optics, a high-resolution polarization-resolved wavefront detector and synthesizer and accurate alignment between them. Effects of noise and other experimental limitations on F are described by Cui and co-workers [13], Yılmaz and co-workers [17] and van Putten and co-workers [18]. Our approach towards maximizing F is described in Chapter 4.

2.3 Coupling light to open channels of strongly scattering media

2.3.1 The scattering and transmission matrices

The transport of light through a multiple-scattering medium can be described by means of the scattering matrix S [1]. We consider a scattering medium in a slab geometry and we call the two sides of the slab the left and right side. Then S relates the fields emerging from the scattering medium to the fields incident on the scattering medium:

$$\begin{pmatrix} E^{\text{l}}_{\text{out}} \\ E^{\text{r}}_{\text{out}} \end{pmatrix} = S \begin{pmatrix} E^{\text{l}}_{\text{in}} \\ E^{\text{r}}_{\text{in}} \end{pmatrix}, \tag{2.1}$$

where E^{l}_{in} and E^{r}_{in} denote the fields incident to the slab from the left and right side, respectively, and $E^{\text{l}}_{\text{out}}$ and $E^{\text{r}}_{\text{out}}$ are the fields that emerge from the slab on

[1] $F = 1$ does not mean 100% of the light goes to the focus, as that can only be achieved by phase conjugating the transmitted and the reflected light simultaneously.

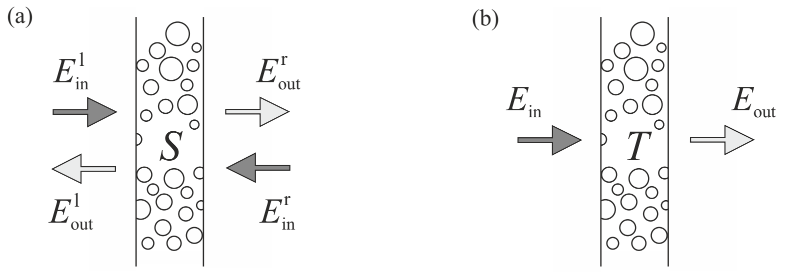


Figure 2.2: (a) The scattering matrix S describes the coupling of incident fields to outgoing fields on both sides of a disordered slab. (b) The transmission matrix T describes the coupling of an incident field on one side of a disordered slab to the outgoing field on the other side. Image from [18].

the left and right side. The coupling between the fields by S is illustrated in Fig. 2.2(a). The scattering matrix S contains four submatrices called the reflection and transmission matrices:

$$S = \begin{pmatrix} R^{\mathrm{ll}} & T^{\mathrm{rl}} \\ T^{\mathrm{lr}} & R^{\mathrm{rr}} \end{pmatrix}, \tag{2.2}$$

where R^{ll} is the reflection matrix on the left side of the slab, R^{rr} is the reflection matrix on the right side of the slab, T^{lr} is the transmission matrix from the left side of the slab to the right side and T^{rl} is the transmission matrix from right to left. Energy conservation requires S to be unitary, from which it immediately follows that T^{lr} and T^{rl} are each other's conjugate transpose: $T^{\mathrm{lr}} = T^{\mathrm{rl}\dagger}$. Therefore, the transmission matrix $T = T^{\mathrm{lr}}$ describes the light transport through the slab in both directions:

$$E^{\mathrm{r}}_{\mathrm{out}} = T E^{\mathrm{l}}_{\mathrm{in}}, \tag{2.3a}$$

$$E^{\mathrm{l}}_{\mathrm{out}} = T^{\dagger} E^{\mathrm{r}}_{\mathrm{in}}. \tag{2.3b}$$

Fig. 2.2(b) illustrates the coupling of an incident field to the transmitted field by T.

2.3.2 Transmission channels

The transmission matrix can be decomposed by use of the singular value decomposition:

$$T = U \Sigma V^{\dagger}, \tag{2.4}$$

where V and U are unitary complex-valued matrices of which the columns are the right and left singular vectors of T, respectively. Σ is a real and positive diagonal matrix containing the singular values of T. The right and left singular vectors are, typically, speckle field patterns and the singular values are field transmission coefficients.

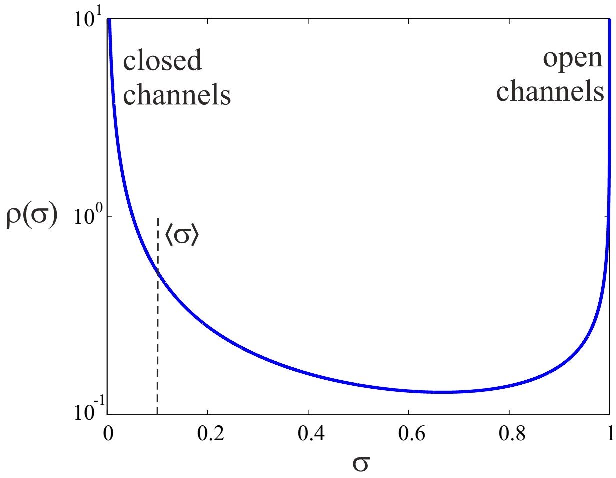


Figure 2.3: Density of transmission channels as function of transmission coefficient for wave transport through a multiple-scattering medium, plotted for an average transmission $\langle\sigma\rangle = 0.1$.

A transmission channel is a combination of a right singular vector and its corresponding singular value and left singular vector. When an arbitrary field E_{in}^{l} is incident on the sample it is first projected onto the right singular vectors, which are contained in V. This projection determines how much light is coupled into each transmission channel. Then, the light transport through each channel is attenuated by the channel's amplitude transmission coefficient, which is an element of Σ. Finally, the light is coupled out of the channel in the channel's specific transmission profile, which is its left singular vector contained in U.

The transmission coefficient distribution of multiple-scattering media is obtained from random matrix theory. Random matrix theory is a field in which physical systems are modeled by large random matrices, allowing statistical investigation of properties of the system [19, 20]. The probability distribution of intensity transmission coefficients through a scattering medium is known as the Dorokhov-Mello-Pereyra-Kumar (DMPK) distribution [1, 21–23] and sometimes called bimodal distribution. The intensity transmission coefficients are the squares of the amplitude transmission coefficients of T: $\sigma \in \Sigma^2$. The distribution was developed for samples with transverse confinement, but theoretical as well as experimental results indicate that it also applies to slab geometries [2, 3]. For a sample with thickness L and transport mean free path[2] l the DMPK distribution is given by

$$f(\sigma) = \frac{\langle\sigma\rangle}{2\sigma\sqrt{1-\sigma}}, \tag{2.5}$$

[2] The transport mean free path l is defined as the average propagation distance after which the light completely loses its direction [24].

starting at a minimum transmission coefficient $\sigma_{\min} \approx \cosh^{-2}(L/l)$ and with an average transmission of $\langle\sigma\rangle \approx l/L$. The distribution diverges at $\sigma \to 1$ and at $\sigma \to 0$ and, therefore, for each channel the probability that it has a very high or very low transmission is relatively high. Channels with very high and very low transmission are called open and closed channels, respectively.

We make the approximation that there is a continuum of channels by taking the limit of the number of channels to infinity. In that case the density ρ of channels as function of transmission is equal to the DMPK distribution: $\rho(\sigma) = f(\sigma)$. The channel density is shown in Fig. 2.3.

The existence of open channels in optical multiple-scattering media was experimentally demonstrated by Vellekoop and Mosk [3]. In their experiment, creating a focus through a multiple-scattering medium by wavefront shaping led to an increase in total transmission of up to 44%. Since then, several groups have tried to maximize the coupling to open channels. In the first transmission matrix measurements Popoff and co-workers measured a singular value distribution and compared it to Marcenko-Pastur theory of small submatrices [25]. Popoff and co-workers enhanced the transmission by a factor of 3.6 by wavefront shaping with total transmission as the feedback signal [26]. Kim and co-workers reported a transmission enhancement by a factor of 3.99 by measuring a partial transmission matrix $\widetilde{T}$, performing the singular value decomposition, and shaping light to couple to the highest transmitting channel of $\widetilde{T}$ [27]. Hao and co-workers report an enhancement of 2.7 by iterative phase conjugation [28].

2.3.3 Ping-pong with light

Our method of choice for optimally coupling light to open channels is iterative phase conjugation, or ping-pong, with light. The advantage of ping-pong over focusing through the medium is that for ping-pong the coupling efficiency has no theoretical limit, whereas it is limited to 2/3 when focusing [3]. The advantage of ping-pong over measuring the complete transmission matrix is that ping-pong requires orders of magnitude fewer measurements, and is therefore much faster. The disadvantage is that only the highest-transmission channel is found, with very limited information on the other channels.

The basic steps of ping-pong with light are shown in Fig. 2.4. The process starts in Fig. 2.4(a) by wavefront synthesizer 1 (S1) creating a wavefront which propagates to the multiple-scattering medium. The wavefront couples to the channels of the scattering medium. After transmission the wavefront is measured by wavefront detector 2 (D2). In Fig. 2.4(b) wavefront synthesizer 2 (S2) synthesizes the conjugate of the wavefront measured by D2, which then propagates back to the scattering medium. The light again passes through the transmission channels and is detected by wavefront detector 1 (D1). S1 again synthesizes the detected wavefront (not shown) and the process is repeated until it converges.

If the phase conjugation fidelity F equals 1, light passing through a transmission channel is always conjugated back into the same transmission channel with 100% efficiency. Therefore, channels can be considered completely independently. Each time light passes through a transmission channel it is attenuated

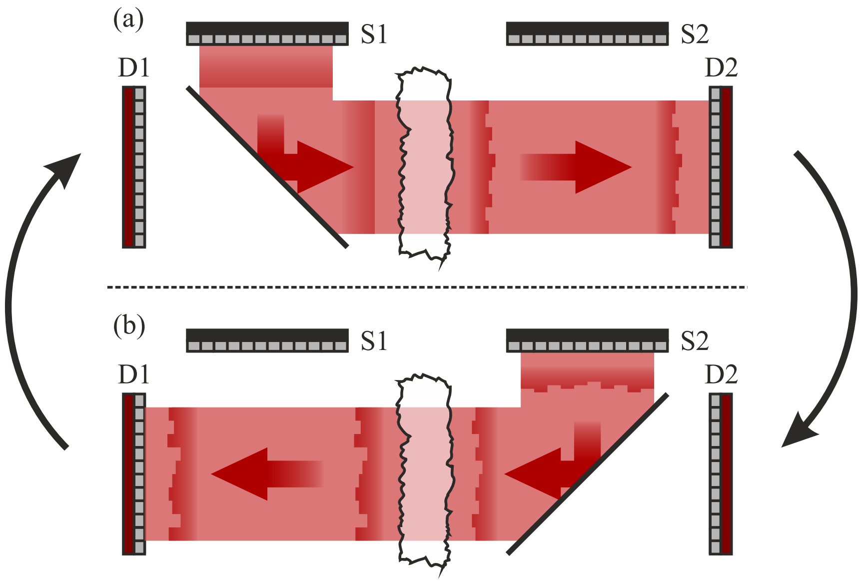


Figure 2.4: Schematic of iterative phase conjugation, or ping-pong, of light. (a) A wavefront constructed by wavefront synthesizer 1 (S1) passes through the multiple-scattering medium and is recorded by wavefront detector 2 (D2) (b) The measured wavefront is phase conjugated by wavefront synthesizer 2 (S2) and sent back through the scattering medium, after which it is detected by wavefront detector 1 (D1). This process is repeated.

by the channel's transmission coefficient σ. After N passes through the channel, the channel's contribution is attenuated by σ^N.

At the start of the ping-pong process the energy on the input side of the sample is distributed equally over all channels, on average. This means that the initial normalized energy per channel on the input side does not depend on the channel's transmission coefficient: $\Phi_0(\sigma) = 1$. The total energy density as function of channel transmission coefficient, which is the quantity we are ultimately interested in, is equal to the energy per channel multiplied by the channel density:

$$I_N(\sigma) = \Phi_N(\sigma)\rho(\sigma). \tag{2.6}$$

It immediately follows that the initial distribution of energy is $I_0(\sigma) = \rho(\sigma)$, i.e. the DMPK distribution. The initial distribution is shown in Fig. 2.5 for an initial average transmission of $\langle\sigma\rangle = 0.1$. Each pass through the medium multiplies the energy in channels with transmission σ by σ: $\widetilde{I}_N(\sigma) = \sigma I_{N-1}(\sigma)$, so that after

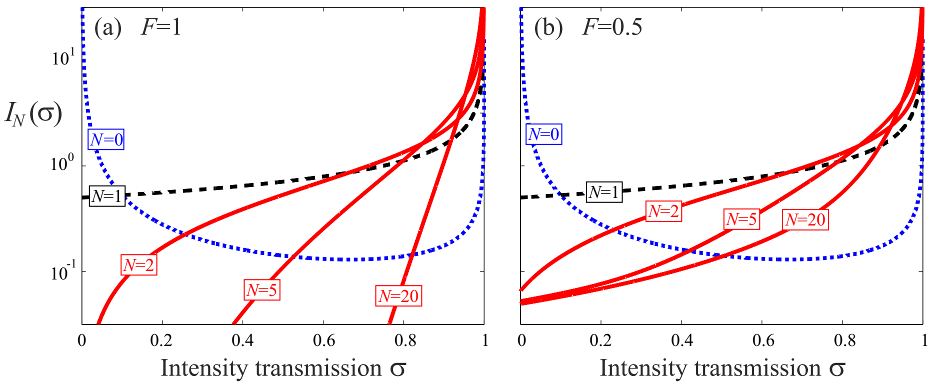


Figure 2.5: Energy distribution as function of transmission coefficient after N passes through the medium (a) for perfect phase conjugation $F = 1$ and (b) for $F = 0.5$. $N = 0$ corresponds to the incident energy distribution at the start of the process. The energy is redistributed towards open channels as the number of iterations N increases. The initial average transmission $\langle\sigma\rangle = 0.1$.

N passes

$$\widetilde{I}_N^{F=1}(\sigma) = \sigma^N I_0(\sigma) = \frac{\langle\sigma\rangle\sigma^{N-1}}{2\sqrt{1-\sigma}}, \tag{2.7a}$$

$$I_N^{F=1}(\sigma) = \frac{\widetilde{I}_N^{F=1}(\sigma)}{\int_0^1 \widetilde{I}_N^{F=1}(\sigma)\mathrm{d}\sigma}, \tag{2.7b}$$

where Eq. 2.7b is a normalization. Several $I_N^{F=1}(\sigma)$ are plotted in Fig. 2.5(a). At $N = 0$ we see that most of the light enters closed channels. At $N = 1$, after one pass, we see that the low-transmission channels are suppressed, but not completely. For increasing N the distribution of energy shifts more and more towards the open channels.

For imperfect phase conjugation, i.e. $F < 1$, ping-pong is less efficient. We assume that the level of control over a channel does not correlate with its transmission coefficient: $F(\sigma) = F$. Then, at each step only a fraction F of the light is correctly phase conjugated back into the channels it passed through before. The remainder of the light is randomly coupled into all channels of the system. The model that we obtain is

$$\widetilde{I}_N(\sigma) = F\sigma I_{N-1}(\sigma) + (1-F)\sigma I_0(\sigma), \tag{2.8a}$$

$$I_N(\sigma) = \frac{\widetilde{I}_N(\sigma)}{\int_0^1 \widetilde{I}_N(\sigma)\mathrm{d}\sigma}. \tag{2.8b}$$

$I_N(\sigma)$ are plotted for $F = 0.5$ in Fig. 2.5(b). We observe that the energy strongly redistributes towards channels with high transmission as N increases, but the suppression of low-transmission channels is lower than for the $F = 1$ case.

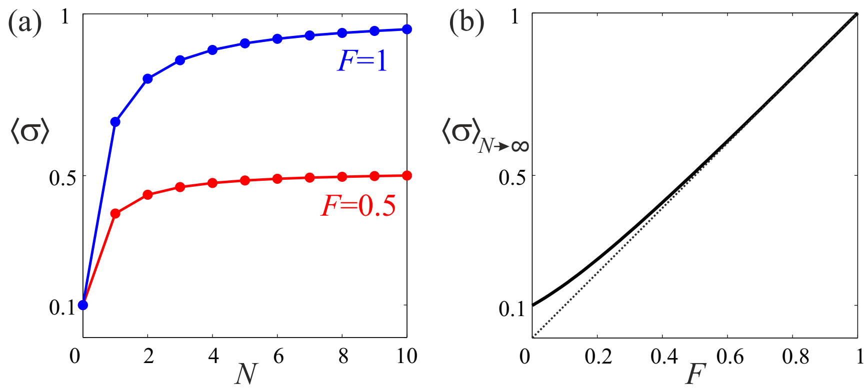


Figure 2.6: (a) Average transmission after N phase conjugation iterations for $F = 0.5$ and $F = 1$. (b) Limit of the average transmission as $N \to \infty$. The dotted line is a guide to the eye.

The average transmission through the sample after N phase conjugation iterations is given by

$$\langle \sigma \rangle_N = \int_0^1 F\sigma I_N(\sigma) + (1-F)\sigma I_0(\sigma) \mathrm{d}\sigma. \tag{2.9}$$

For $F = 1$ Eq. 2.9 simplifies and has the analytical solution

$$\langle \sigma \rangle_N^{F=1} = \frac{2N}{1+2N}. \tag{2.10}$$

This equation holds for $N \geq 1$ and does not depend on the initial average transmission. For $N = 1$ the universal conductance of 2/3 [3] is retrieved and the total transmission converges to 1 for $N \to \infty$. For $F < 1$ Eq. 2.9 is solved numerically. The average transmission as function of N is plotted in Fig. 2.6(a) for $F = 1$ and $F = 0.5$. In both cases we observe convergence to a value close to the apparent maximum in approximately 10 iterations. In Fig. 2.6(b) we plot the maximum achievable transmission as function of F for a scattering medium with an initial average transmission of 0.1. The maximum transmission is approximately equal to F. Scattering media with low initial transmission show similar behavior. This indicates that ping-pong with light can make the transmission very high, namely of order F, even for samples with a very low initial transmission.

2.3.4 Comparison to partial transmission matrix model

Our approach to taking into account incomplete control over the channels is a radical departure from what is assumed in transmission matrix models. Let us assume that the level of control $F = \frac{m}{M}$ is equal to the fraction of the solid angle that is controlled and is determined by the limited NA of the microscope objectives. In such situation the common thing to do is to consider the transmission coefficient distribution of the partial transmission matrix that is experimentally accessible [26–30].

The power of our approach becomes clear when we make a comparison between the two models for $m \ll M$. For small m, and assuming the same degree of control on both sides of the sample, the transmission coefficients of the partial transmission matrix follow a quarter-circle distribution [31] with a maximum intensity transmission coefficient $\sigma_{\max} = 4\langle\sigma\rangle$. This implies that even for very small m it is possible to enhance transmission by a factor of 4, either by performing ping-pong (following [28]) or by measuring the partial transmission matrix (similar to [27]). This enhancement, however, is a transmission enhancement of the detected light. No immediate conclusion can be drawn regarding enhancement of the undetected transmission channels. Therefore, it is unclear whether the total transmission is increased.

Our model takes into account all channels of the sample, rather than only the ones in the partial transmission matrix. Therefore, it provides insight into the enhancement of the total transmission. From the combined models we conclude that in the limit $\frac{m}{M} \to 0$ ping-pong may allow a strong redistribution of transmitted intensity without enhancing total transmission. This is similar to results obtained by wavefront shaping [3] and we expect the same to hold when coupling light to an open channel of a small partial transmission matrix.

2.4 Coupling light to long-lived modes of strongly scattering media

In multiple wave scattering two regimes are distinguished: the diffuse regime and the Anderson localized regime [32, 33]. In the diffuse regime, fields are extended throughout the multiple-scattering medium. In the localized regime, on the other hand, fields typically have a small spatial extent. Fields in the localized regime are, approximately, standing wave solutions of the Maxwell equations and decay, on average, exponentially with distance from their centers. We call a localized field a mode of the system, although the term quasimode would be more appropriate considering the dissipation induced by the finite size of the system. Localized modes are isolated in frequency space and have linewidths that directly correspond to their leakage out of the system. The Anderson localized regime is predicted for strongly scattering media with $kl_{\mathrm{tr}} < 1$, where k is the wavevector of the light and l_{tr} is the transport mean free path. Close to the localized regime an intermediate regime is predicted in which extended and localized modes coexist [4, 5, 34, 35]. In this regime localized modes that overlap in frequency are likely to hybridize and form necklace states [36]. No clear observations of localized modes for vector fields in 3D disordered media have been reported to date. In principle, random lasers are suitable for identifying localized modes, but the extra experimental complexity induced by introducing a gain medium and pumping it complicates interpretation of the results [37]. In this section we propose an alternative method for elucidating the mode structure of strongly scattering disordered media.

The transmission of light through a multiple-scattering medium in slab geometry can be described in the frequency domain as

$$E_{\mathrm{out}}(x,y,\omega)=\int\int G(x,y,x',y',\omega)S_{\mathrm{in}}(x',y',\omega)\mathrm{d}x'\mathrm{d}y', \tag{2.11}$$

where S_{in} is a source term representing the incident field, E_{out} is the transmitted field on the opposite surface and G is the Green function which relates the transmitted field to the source. In the presence of isolated resonant modes the Green function can be decomposed into

$$G(x,y,x',y',\omega)=\sum_{\mathrm{n}} u_{\mathrm{n}}(x,y)f_{\mathrm{n}}(\omega)v_{\mathrm{n}}(x',y')+\widetilde{G}(x,y,x',y',\omega), \tag{2.12}$$

where n is the resonant mode index, v_{n} and u_{n} are the mode profiles on the input and output surfaces of the slab, respectively, f_{n} is the frequency profile of the mode and $\widetilde{G}$ is a collection term for the remaining part of the Green function. The frequency profiles of isolated resonant modes have a Lorentzian shape [38]

$$f_{\mathrm{n}}(\omega)=\frac{\Gamma_{\mathrm{n}}/2}{\Gamma_{\mathrm{n}}/2+i(\omega-\omega_{\mathrm{n}})}, \tag{2.13}$$

where ω_{n} is the central frequency of the mode and Γ_{n} is the linewidth of the mode. We assume a non-absorbing system, so that when a mode with linewidth Γ_{n} is excited it decays in time $\tau_n=2/\Gamma_{\mathrm{n}}$ due to leakage out of the system. The distribution of mode lifetimes in 3D strongly scattering media is not known [39]. We describe a method for finding the mode with the largest decay time, which may prove to be an important tool for experimentally investigating the decay time distribution in multiple-scattering media.

Our method to find the longest-lived mode assumes an unknown mode lifetime density distribution $\rho(\tau)$ cut off at a maximum lifetime τ_{max}, making the implicit approximation that there is a continuum of modes. We also assume that when the sample is illuminated by an arbitrary initial field all modes are excited equally: $\Phi_0(\tau)=1$. The total energy coupling to modes with lifetime τ, which is the quantity we are interested in, equals the energy per mode multiplied by the mode density:

$$I(\tau)=\Phi(\tau)\rho(\tau). \tag{2.14}$$

We start by illuminating the sample with an arbitrary initial field, for which the energy distribution $I_0(\tau)=\rho(\tau)$, and measure the frequency derivative $\frac{\mathrm{d}E_{\mathrm{out}}(x,y,\omega)}{\mathrm{d}\omega}$ or $\frac{\mathrm{d}^2E_{\mathrm{out}}(x,y,\omega)}{\mathrm{d}\omega^2}$ of the transmitted field. The frequency derivatives of Eq. 2.13 are given by

$$\frac{\mathrm{d}f_{\mathrm{n}}(\omega)}{\mathrm{d}\omega}=\frac{-\mathrm{i}\Gamma_{\mathrm{n}}/2}{(\Gamma_{\mathrm{n}}/2+i(\omega-\omega_{\mathrm{n}}))^2}, \tag{2.15a}$$

$$\frac{\mathrm{d}^2f_{\mathrm{n}}(\omega)}{\mathrm{d}\omega^2}=\frac{-\Gamma_{\mathrm{n}}}{(\Gamma_{\mathrm{n}}/2+i(\omega-\omega_{\mathrm{n}}))^3}. \tag{2.15b}$$

Close to resonance $|\omega - \omega_n| \ll \Gamma_n$ we find that the contributions of the modes are amplified by $2/\Gamma_n$ when taking the first derivative and by $2/\Gamma_n^2$ when taking the second derivative. This indicates that modes with small Γ_n, i.e. long lifetime $\tau_n = 2/\Gamma_n$, are strongly amplified, so that the contributions to $\frac{dE_{out}(x,y,\omega)}{d\omega}$ and $\frac{d^2E_{out}(x,y,\omega)}{d\omega^2}$ from long-lived modes are strongly enhanced compared to the contributions from other modes. Therefore, we phase conjugate $\frac{dE_{out}(x,y,\omega)}{d\omega}$ or $\frac{d^2E_{out}(x,y,\omega)}{d\omega^2}$ and illuminate the sample with it in order to obtain more efficient coupling to long-lived modes. In case the field that is sent back at each phase conjugation iteration N is the first derivative of the measured field,

$$E_{out}^{N}(x,y,\omega) = \frac{dE_{out}^{N-1}(x,y,\omega)}{d\omega}, \tag{2.16}$$

the model predicts that

$$I_N(\tau) = F\frac{\tau^2 I_{N-1}(\tau)}{\int_0^{\tau_{max}} \tau^2 I_{N-1}(\tau)d\tau} + (1-F)I_0(\tau), \tag{2.17}$$

where F is the phase conjugation fidelity, τ_{max} is the lifetime of the longest-lived mode in the system and the energy distribution is normalized at each iteration. The field enhancement by a factor $2/\Gamma = \tau$ in Eq. 2.15a leads to an energy enhancement of τ^2 in Eq. 2.17. We assume that the level of control over a mode does not depend on its lifetime, $F(\tau) = F$, so that the uncontrolled fraction $1-F$ of the energy is, on average, uniformly distributed over all modes in the system.

The method described here is effectively ping-pong with the Smith-Purcell lifetime matrix [40, 41]. It is expected to enhance the coupling of light to the longest-lived states of systems of any scattering strength.

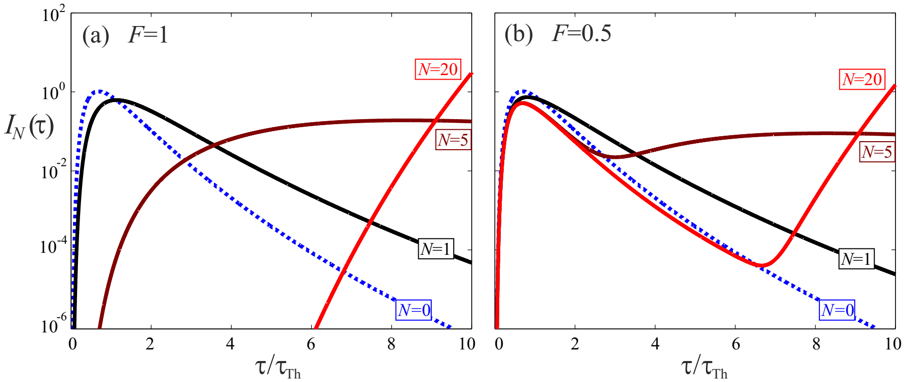


Figure 2.7: Energy distribution as function of lifetime (a) for perfect phase conjugation $F = 1$ and (b) for $F = 0.5$. $N = 0$ corresponds to the test energy distribution incident to the sample at the start of the process. The energy is redistributed towards the mode with the longest lifetime as the number of iterations N increases.

A test distribution of lifetimes can be used to evaluate the method. The test distribution $\rho(\tau)$ that we choose is lognormal, noting that the tail of the distribution is predicted to show lognormal decay [4]. The test distribution has a cut off at an arbitrary maximum lifetime $\tau_{\max} = 10\tau_{\mathrm{Th}}$, where $\tau_{\mathrm{Th}} = L^2/D$ is the Thouless time, $D = \frac{1}{3}v_{\mathrm{E}}l_{\mathrm{tr}}$ is the diffusion constant and v_{E} is the transport velocity [42]. Eq. 2.17 is solved numerically and the result is shown in Fig. 2.7 for $F = 1$ and $F = 0.5$. The initial distribution of energy as function of mode lifetime $I_0(\tau) = \rho(\tau)$ is shown by the dashed curves at $N = 0$. We observe for $F = 1$ as well as $F = 0.5$ that as the number of phase conjugation iterations N increases, the energy distribution shifts towards the longest-lived modes in the system.

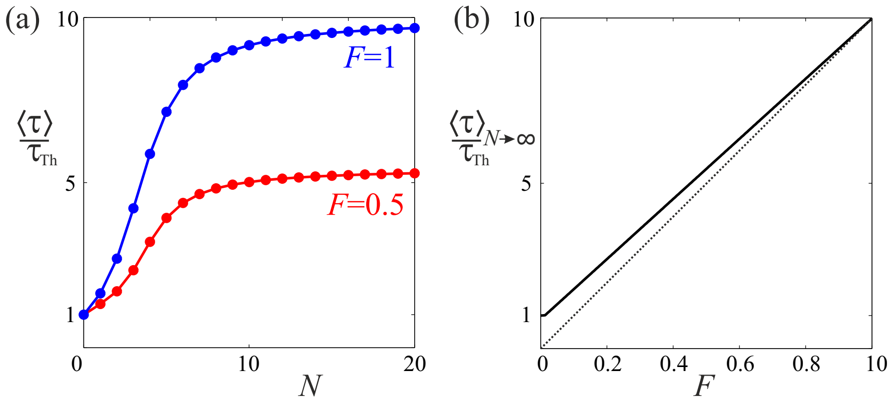


Figure 2.8: (a) Average lifetime after N iterations for $F = 0.5$ and $F = 1$ for a scattering medium with a maximum lifetime of $10\tau_{\mathrm{Th}}$. (b) Limit of the average lifetime as $N \to \infty$. The dashed line is a guide to the eye.

The convergence of the process is shown in Fig. 2.8. In Fig. 2.8(a) we see that the process converges to an average lifetime of approximately $10\tau_{\mathrm{Th}}$ for $F = 1$ and an average lifetime of more than $5\tau_{\mathrm{Th}}$ for $F = 0.5$. We see that the convergence speeds up after the first few phase conjugation iterations and that the fastest increase in average lifetime occurs after approximately 4 iterations. The process stabilizes after approximately 10 iterations. Simulations with other test distributions show that the convergence speed depends on the level of suppression of long-lived modes in the initial distribution: if long-lived modes are initially suppressed more, it takes longer to purify them. However, in several numerical simulations we observed that convergence to a coupling of a fraction F of the light to the longest-lived modes always occurs, independent from the initial suppression of the longest-lived modes. Fig. 2.8(b) shows the average lifetime for $N \to \infty$. The numerical data follows the linear relation $\langle\tau\rangle_{N\to\infty} = F\tau_{\max} + (1-F)\tau_{\mathrm{Th}}$, indicating that a fraction F of the light is coupled to the longest-lived mode in the system.

It is expected that a system with phase conjugation fidelity F cannot couple more than a fraction F of the light into the longest-lived mode in the system.

From this point of view, taking first derivatives seems to achieve the optimal result. However, Eq. 2.15b shows that taking second derivatives more strongly amplifies long-lived modes than the first derivatives that we considered until now. Therefore, assuming equal F, the convergence is expected to be faster when taking second derivatives. However, experimentally taking higher order derivatives typically increases noise and therefore may reduce F.

The experiment described in this section is fundamentally different from recently reported results [43–45], in which light is focused at selected points in time. The coupling of light to long-lived modes, as described here, enhances the transmission at all long times and delays the all-angle average time after which light transmits through the sample. From the focusing experiments, on the other hand, no immediate conclusions can be drawn regarding the average time delay of the transmitted light.

2.5 Summary

In this chapter we have investigated two phenomena in multiple-scattering media: open channels and long-lived modes. We proposed and analyzed methods for identification of and coupling to open channels and long-lived modes. Our model takes into account all channels and modes of the system, without restricting ourselves to the experimentally accessible part of the system. This enables predictions on for example the *overall* enhancement of the total transmission and of the time light spends inside the scattering medium. Numerical results show that the methods rapidly converge to a highly efficient coupling to open channels and the longest-lived mode in the system, only limited by the phase conjugation fidelity F of the apparatus. Even for moderate F, efficient coupling to open channels and long-lived modes occurs. These very promising predictions form a basis for experiments to be carried out using the apparatus described in Chapter 4.

Bibliography

[1] C. W. J. Beenakker, *Random-matrix theory of quantum transport*, Rev. Mod. Phys. **69**, 731 (1997). — p.13, 15, 17.

[2] Y. V. Nazarov, *Limits of universality in disordered conductors*, Phys. Rev. Lett. **73**, 134 (1994). — p.13, 17.

[3] I. M. Vellekoop and A. P. Mosk, *Universal optimal transmission of light through disordered materials*, Phys. Rev. Lett. **101**, 120601 (2008). — p.13, 17, 18, 21, 22.

[4] B. L. Al'tshuler, V. E. Kravtsov, and I. V. Lerner, *Spectrum of relaxation times in disordered conductors*, JETP Lett. **45**, 199 (1987). — p.13, 22, 25.

[5] V. M. Apalkov, M. E. Raikh, and B. Shapiro, *Random resonators and prelocalized modes in disordered dielectric films*, Phys. Rev. Lett. **89**, 016802 (2002). — p.13, 22.

[6] K. Vynck, M. Burresi, F. Riboli, and D. S. Wiersma, *Photon management in two-dimensional disordered media*, Nature Mater. **11**, 1017 (2012). — p.13.

[7] E. N. Leith and J. Upatnieks, *Holographic imagery through diffusing media*, J. Opt. Soc. Am. **56**, 523 (1966). — p.14.

[8] R. K. Tyson, *Principles of adaptive optics*, 2nd ed. (Academic Press, New York, U.S.A., 1998). — p.14.

[9] J. M. Beckers, P. Léna, O. Lai, P.-Y. Madec, G. Rousset, M. Séchaud, M. J. Northcott, F. Roddier, J.-L. Beuzit, F. Rigaut, and D. G. Sandler, in *Adaptive optics in astronomy*, edited by F. Roddier (Cambridge University Press, Cambridge, U.K., 1999). — p.14.

[10] I. M. Vellekoop and A. P. Mosk, *Focusing coherent light through opaque strongly scattering media*, Opt. Lett. **32**, 2309 (2007). — p.14.

[11] Z. Yaqoob, D. Psaltis, M. S. Feld, and C. Yang, *Optical phase conjugation for turbidity suppression in biological samples*, Nature Photon. **2**, 110 (2008). — p.14.

[12] C. L. Hsieh, Y. Pu, R. Grange, and D. Psaltis, *Digital phase conjugation of second harmonic radiation emitted by nanoparticles in turbid media*, Opt. Express **18**, 12283 (2010). — p.14.

[13] M. Cui and C. Yang, *Implementation of a digital optical phase conjugation system and its application to study the robustness of turbidity suppression by phase conjugation*, Opt. Express **18**, 3444 (2010). — p.14, 15.

[14] D. M. Pepper, *Nonlinear optical phase conjugation*, Opt. Eng. **21**, 156 (1982). — p.14.

[15] H. J. Gerritsen, *Nonlinear effects in image formation*, Appl. Phys. Lett. **10**, 239 (1967). — p.14.

[16] J. P. Woerdman, *Formation of a transient free carrier hologram in Si*, Opt. Commun. **2**, 212 (1970). — p.14.

[17] H. Yılmaz, W. L. Vos, and A. P. Mosk, *Optimal control of light propagation through multiple-scattering media in the presence of noise*, Biomed. Opt. Express **4**, 1759 (2013). — p.15.

[18] E. G. van Putten, *Disorder-enhanced imaging with spatially controlled light*, Ph.D. thesis, University of Twente, 2011. — p.15, 16.

[19] P. J. Forrester, N. C. Snaith, and J. J. M. Verbaarschot, *Developments in random matrix theory*, J. Phys. A: Math. Gen. **36**, R1 (2003). — p.17.

[20] M. L. Mehta, *Random matrices* (Elsevier Academic Press online book, 2004). — p.17.

[21] O. N. Dorokhov, *Transmission coefficient and the localization length of an electron in N bound disordered chains*, JETP Lett. **36**, 318 (1982). — p.17.

[22] O. N. Dorokhov, *On the coexistence of localized and extended electronic states in the metallic phase*, Solid State Commun. **51**, 381 (1984). — p.17.

[23] P. A. Mello, P. Pereyra, and N. Kumar, *Macroscopic approach to multichannel disordered conductors*, Ann. Phys. **181**, 290 (1988). — p.17.

[24] M. C. W. van Rossum and T. M. Nieuwenhuizen, *Multiple scattering of classical waves: microscopy, mesoscopy, and diffusion*, Rev. Mod. Phys. **71**, 313 (1999). — p.17.

[25] S. M. Popoff, G. Lerosey, R. Carminati, M. Fink, A. C. Boccara, and S.

Gigan, *Measuring the transmission matrix in optics: an approach to the study and control of light propagation in disordered media*, Phys. Rev. Lett. **104**, 100601 (2010). — p.18.

[26] S. M. Popoff, A. Goetschy, S. F. Liew, A. D. Stone, and H. Cao, *Coherent control of total transmission of light through disordered media*, Phys. Rev. Lett. **112**, 133903 (2014). — p.18, 22.

[27] M. Kim, Y. Choi, C. Yoon, W. Choi, J. Kim, Q.-H. Park, and W. Choi, *Maximal energy transport through disordered media with the implementation of transmission eigenchannels*, Nature Photon. **6**, 581 (2012). — p.18, 22.

[28] X. Hao, L. Martin-Rouault, and M. Cui, *A self-adaptive method for creating high efficiency communication channels through random scattering media*, Sci. Rep. **4**, 5874 (2014). — p.18, 22.

[29] A. Goetschy and A. D. Stone, *Filtering random matrices: the effect of imperfect channel control in multiple-scattering*, Phys. Rev. Lett. **111**, 063901 (2013). — p.22.

[30] D. Akbulut, *Measurements of strong correlations in the transport of light through strongly scattering materials*, Ph.D. thesis, University of Twente, 2013. — p.22.

[31] V. A. Marčenko and L. A. Pastur, *Distribution of eigenvalues for some sets of random matrices*, Math. USSR Sb. **1**, 457 (1967). — p.22.

[32] P. W. Anderson, *Absence of diffusion in certain random lattices*, Phys. Rev. **109**, 1492 (1958). — p.22.

[33] A. Lagendijk, B. A. van Tiggelen, and D. S. Wiersma, *Fifty years of Anderson localization*, Phys. Today **62**, 24 (2009). — p.22.

[34] A. A. Chabanov, Z. Q. Zhang, and A. Z. Genack, *Breakdown of diffusion in dynamics of extended waves in mesoscopic media*, Phys. Rev. Lett. **90**, 203903 (2003). — p.22.

[35] C. Vanneste and P. Sebbah, *Complexity of two-dimensional quasimodes at the transition from weak scattering to Anderson localization*, Phys. Rev. A **79**, 041802 (2009). — p.22.

[36] K. Y. Bliokh, Y. P. Bliokh, V. Freilikher, A. Z. Genack, B. Hu, and P. Sebbah, *Localized modes in open one-dimensional dissipative random systems*, Phys. Rev. Lett. **97**, 243904 (2006). — p.22.

[37] H. E. Türeci, L. Ge, S. Rotter, and A. D. Stone, *Strong interactions in multimode random lasers*, Science **320**, 643 (2008). — p.22.

[38] A. Z. Genack and S. Zhang, in *Tutorials in complex photonic media, Chapter 9: Wave interference and modes in random media*, edited by M. A. Noginov, G. Dewar, M. W. McCall, and N. I. Zheludev (SPIE Press, Bellingham, Washington, U.S.A., 2009). — p.23.

[39] S. E. Skipetrov and I. M. Sokolov, *Absence of Anderson localization of light in a random ensemble of point scatterers*, Phys. Rev. Lett. **112**, 023905 (2014). — p.23.

[40] F. T. Smith, *Lifetime matrix in collision theory*, Phys. Rev. **118**, 349 (1960). — p.24.

[41] S. Rotter, P. Ambichl, and F. Libisch, *Generating particlelike scattering states in wave transport*, Phys. Rev. Lett. **106**, 120602 (2011). — p.24.

[42] M. P. van Albada, B. A. van Tiggelen, A. Lagendijk, and A. Tip, *Speed of propagation of classical waves in strongly scattering media*, Phys. Rev. Lett. **66**, 3132 (1991). — p.25.

[43] J. Aulbach, B. Gjonaj, P. M. Johnson, A. P. Mosk, and A. Lagendijk, *Control of light transmission through opaque scattering media in space and time*, Phys. Rev. Lett. **106**, 103901:1 (2011). — p.26.

[44] O. Katz, E. Small, Y. Bromberg, and Y. Silberberg, *Focusing and compression of ultrashort pulses through scattering media*, Nature Photon. **5**, 372 (2011). — p.26.

[45] D. J. McCabe, A. Tajalli, D. Austin, P. Bondareff, I. A. Walmsley, S. Gigan, and B. Chatel, *Spatio-temporal focusing of an ultrafast pulse through a multiply scattering medium*, Nat. Commun. **2**, 447 (2011). — p.26.

CHAPTER 3

Superpixel method for spatial amplitude and phase modulation with a digital micromirror device

We present a superpixel method for full spatial phase and amplitude control of a light beam using a digital micromirror device (DMD) combined with a spatial filter. We combine square regions of nearby micromirrors into superpixels by low pass filtering in a Fourier plane of the DMD. At each superpixel we are able to independently modulate the phase and the amplitude of light, while retaining a high resolution and the very high speed of a DMD. The method achieves a measured fidelity $F = 0.98$ for a target field with fully independent phase and amplitude at a resolution of 8×8 pixels per diffraction limited spot. For the $\mathbf{LG}_{10}$ orbital angular momentum mode the calculated fidelity is $F = 0.99993$, using 768×768 DMD pixels. The superpixel method reduces the errors when compared to the state of the art Lee holography method for these test fields by 50% and 18%, with a comparable light efficiency of around 5%. Our control software is publicly available.

3.1 Introduction

Full control over light allows many exciting applications. By tailoring light fields we can now use optics to obtain a great level of control over particles [1]. Shaping light waves greatly improves our ability to see the world around us through optical microscopy [2–5] and allows exciting technologies in the field of optical communication, crucial to support the quantity and security of the rapidly expanding amount of information that is sent around the world [6].

Wavefront shaping allows compensation for and exploitation of scattering due to spatial inhomogenieties in the refractive index of a material [7]. In this way it is possible to image through [8, 9] and inside [10–14] opaque materials, which is of great importance in biomedical imaging. Light propagating through an opaque material can be controlled in time by spatially shaping the incident wavefront [15–17] with applications such as pulse compression. Wavefront shaping also

This chapter has been published as: S.A. Goorden, J.Bertolotti, and A.P. Mosk, Opt. Express **22**, 17999–18009 (2014)

allows the use of multiple-scattering media as a tunable wave plate [18, 19], spectral filter [20, 21] or tunable beamsplitter [22]. The digital micromirror device (DMD) [23] is an excellent candidate for controlling light fields, as it has a very high number of spatial degrees of freedom, a very high framerate, it operates in a broad wavelength range and it is relatively cheap. Each pixel of a DMD is a mirror which can be in one of two positions, corresponding to the 'on' and 'off' states of the pixels. Wavefronts can be controlled using binary amplitude modulation [24], but less efficiently than using phase modulation [8]. Shaping complex fields with binary masks is of continuous interest [25–27], adding to the momentum of the rapidly growing field of computer-generated holography. For reviews see [28–30]. The most common technique to obtain phase modulation with a DMD is Lee holography [31] and has been shown to allow for efficient and fast wavefront shaping [32]. Lee holography in its more general form [31] allows full field control [33]. Lee holography with pixel dithering has been demonstrated and the obtained errors are at the 5% level for low resolution fields [34]. A method has been proposed, but not yet demonstrated, that is based on a complex high spatial resolution Fourier mask and is from an information theoretic point of view optimal [35], but requires involved optics and is not robust to misalignment. We propose and demonstrate a superpixel-based [36] phase and amplitude modulation method, which is highly robust and easy to use while offering full spatial control over the phase and amplitude of a light field. The method is applied, through calculations as well as measurements, to two target fields of high practical relevance: the LG_{10} orbital angular momentum mode and a high resolution field with fully independent amplitude and phase. The modulation accuracy of the method is quantified by calculating the fidelity $F = \left|E^*_{\mathrm{target}} E_{\mathrm{obtained}}\right|^2$ and the error $\delta = 1 - F$, where E_{target} is a target field and E_{obtained} is the field that is obtained using the DMD. The fidelity of the superpixel method is found to be very high in theory as well as in experiments.

3.2 Setup

Our setup is designed to obtain full spatial control over the phase and amplitude of light in one specific plane, which we call the target plane. The field behind the target plane follows from usual beam propagation methods. Our Vialux V4100 DMD with a resolution of 1024×768 pixels and pixel pitch of 13.68μm is imaged onto the target plane using two lenses in a 4f-configuration, as illustrated in Fig. 5.1(a). The lenses are placed slightly off-axis with respect to each other, resulting in an extra phase factor in the target plane. This means that the phase of the target plane response of a DMD pixel depends on the position of the pixel on the DMD. The DMD is divided into superpixels: square groups of $n \times n$ micromirrors. The lenses are placed in such a way that the phase prefactors of the micromirrors within each superpixel are distributed uniformly between 0 and 2π. A spatial filter in the form of a circular aperture is placed in the Fourier plane in between the lenses. The spatial filter blocks the high spatial frequencies so that individual DMD pixels cannot be resolved. The images of the pixels in the target plane are

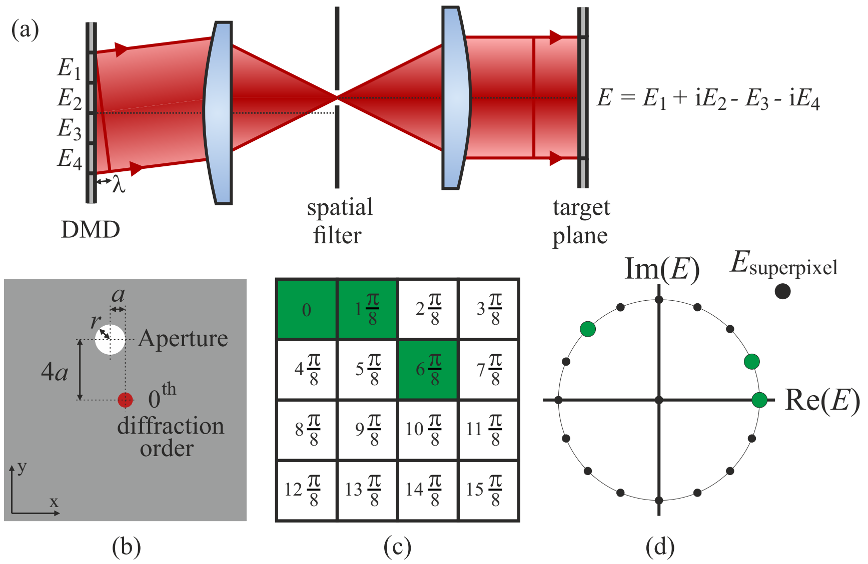


Figure 3.1: (a) In the DMD plane the light field $E(\mathbf{x}) \in \{0, 1\}$, corresponding to the off and on states of the micromirrors. The DMD is imaged onto the target plane in which we maximize the level of control over the light field. The DMD pixel images in the target plane have different phase prefactors, because the lenses are placed off-axis with respect to each other. A low pass filter blurs the images of pixels and averages over groups of neighboring pixels. (b,c,d) The aperture is positioned such that the phase responses of the 16 DMD pixels within a 4×4 superpixel are uniformly distributed between 0 and 2π. Example: if we turn on the three pixels indicated by green squares in (c), then the response $E_{\text{superpixel}}$ in the target plane is the sum of the three pixel responses in (d).

blurred and have a large spatial overlap [36]. Therefore, the target plane response of a superpixel is the sum of the individual pixel responses.

For superpixels of size $n \times n$ the position of the spatial filter with respect to the 0^{th} diffraction order is chosen $(x, y) = (-a, n\ a)$, where $a = \frac{-\lambda f}{n^2 d}$, λ is the wavelength of the light, f is the focal length of the first lens and d is the distance between neighbouring micromirrors. This position is chosen such that the target plane responses of neighbouring pixels inside the superpixel are $\frac{2\pi}{n^2}$ out of phase in the x-direction and $\frac{2\pi}{n}$ out of phase in the y-direction. The target plane responses of the n^2 pixels that make up a superpixel are then uniformly distributed over a circle in the complex plane. For superpixels of size $n = 4$ this is illustrated in Figs. 5.1(b)–5.1(d). Using our DMD, a HeNe laser with a wavelength of $\lambda = 633$ nm and a first lens with a focal length $f_1 = 300$ mm, the aperture is positioned at $(x, y) = (-0.87, 3.47)$ mm. Therefore, the target plane responses of neighbouring pixels in the x and y direction are $\frac{\pi}{8}$ and $\frac{\pi}{2}$ out of phase, as illustrated in Fig. 5.1(c). The phase responses in the target plane of the 16 DMD pixels are then

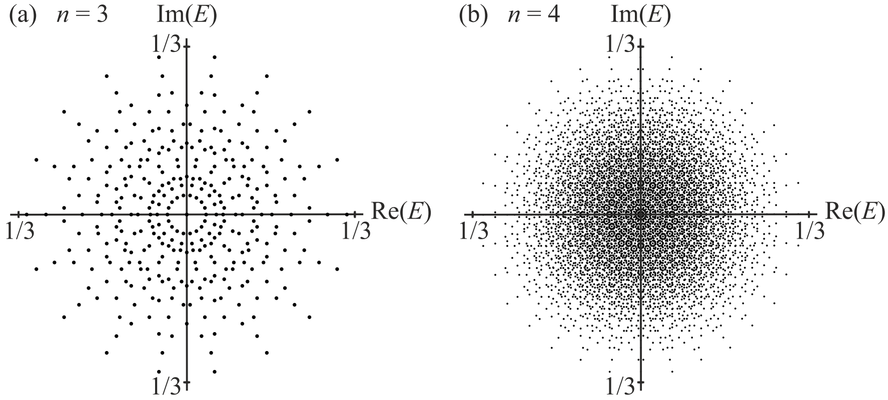


Figure 3.2: (a) Complex target fields that can be constructed using a single superpixel of size 3 × 3. 343 different fields can be constructed. (b) Complex target fields that can be constructed using a single superpixel of size 4 × 4. 6561 different fields can be constructed. Fields are normalized to the incident field. The symbol size is larger for $n = 3$ to increase visibility.

distributed uniformly between 0 and 2π, as shown in Fig. 5.1(d), indicating that we have achieved control over the phase of light.

As an example, we set a superpixel such that the pixels with phase responses 0, $\frac{\pi}{8}$ and $\frac{6\pi}{8}$ are turned on, indicated in Fig. 5.1(c). All other pixels are turned off. The resulting field $E_{\text{superpixel}}$ in the target plane will be approximately equal to the sum of the three dots in Fig. 5.1(d). By turning on different combinations of pixels in a superpixel we can create different target fields in the target plane. For all possible combinations of pixels we plot the corresponding target fields in Fig. 5.2. For superpixels of size $n = 3$ we see in Fig. 5.2(a) that we can construct a total number of 343 different fields, quite uniformly distributed over a disk in the complex plane. For superpixels of size $n = 4$ we see in Fig. 5.2(b) that the number of fields we can construct increases dramatically to 6561, allowing us to create any field within a disk up to a very small discretisation error.

The resolution, or spatial bandwidth, of the superpixel method is given by $\Delta k = \frac{2\pi r}{\lambda f_2}$ rad $\cdot$ m^{-1}, where r is the radius of the aperture and f_2 is the focal length of the second lens. The target plane is an image plane of the DMD and therefore it is natural to express the resolution in units of DMD pixels: $\Delta k' = \frac{2\pi d r}{\lambda f_1}$ rad $\cdot$ pixel^{-1}. We typically choose r such that our system bandwidth matches the bandwidth of the target field, with an upper limit such that the highest allowed spatial frequency is not higher than $\frac{\pi}{2n}$ rad $\cdot$ pixel^{-1}. This upper limit ensures that the images of DMD pixels are blurred and average out to the desired superpixel field value [36]. In our system with superpixel size $n = 4$ the maximum aperture size is $r = 0.9$ mm and the corresponding feature size in the target plane is approximately 2 × 2 superpixels.

Alignment of the spatial filter is done in two steps. First, we write a pattern to the DMD which corresponds to a plane wave in the target plane. The spatial filter is placed around the first diffraction order of this grating. Second, we fine-tune the position and size of the spatial filter by writing horizontal and vertical gratings to the DMD that correspond to the desired spatial band limit of the system. We align the spatial filter such that the two diffraction orders of each grating exactly pass through at the edge of the filter. The DMD patterns for these alignment gratings, as well as for any other target field, are calculated using our superpixel control software [37]. Using this method accurate alignment of the spatial filter is easily achieved. The effect of misalignment of the filter on the resulting light field depends on the spatial frequency distribution of the target field, but is typically small: e.g. 10% relative displacement of the spatial filter results in less than 0.5% loss of modulation fidelity for test field 2.

3.3 Efficiency, bandwidth and implementation

The efficiency of the superpixel method is equal to the maximum intensity a superpixel can create. The maximum intensity is obtained by turning on exactly half of the pixels in a superpixel, e.g. the upper 8 pixels in Fig. 5.1(c). This coincides with the maximum amplitude in Fig. 5.2(b). The calculated efficiency of the modulation method is then 10.3% of the incident intensity. The measured 0 order diffraction efficiency of the DMD itself is 60% for our DMD and our measured modulation efficiency is 7%. The total measured efficiency of our implementation of the superpixel method is 4%. This is similar to the efficiency of Lee holography, since both methods are based on filtering out the first order of an intensity diffraction grating.

Wavelength dispersion of the amplitude mask formed by the DMD limits the frequency bandwidth in which the superpixel method works. The superpixel-based phase and amplitude modulation method can be set up for any wavelength λ at which the DMD functions. The position and size of the spatial filter depend on λ. Illuminating the DMD with light of a different wavelength, e.g. $\lambda + \Delta\lambda$, decreases the modulation fidelity. The error induced in the target plane is, to first order, a phase gradient added to the target field. The period of the phase gradient is equal to $|n\lambda/\Delta\lambda|$ DMD pixels. For DMD chips of approximately 1000 pixels this phase gradient is significant for $|\Delta\lambda/\lambda| > 0.1\%$. However, apart from this phase gradient the obtained field has a high fidelity until $|\Delta\lambda/\lambda| \approx 10\%$, at which point the field in the Fourier plane is so much displaced that the light starts to miss the spatial filter.

A lookup table is used to make the connection between the desired target field at a superpixel and the combination of pixels within the superpixel that should be turned on in order to create that field. By using a lookup table the calculations needed to determine which DMD pixels to turn on are minimized and therefore the performance is optimized. We define a sufficiently fine square grid of possible target fields in the complex plane. We create a lookup table which contains for every point on this grid the nearest field the superpixel method can create as well as the combination of pixels that should be turned on in order to create this field. The size of the lookup table is chosen to be 855 × 855 points, about 100 times more dense than the set of possible target fields at superpixel size $n = 4$. In our implementation it takes under 4 MB of memory to store the table. Loading the table and using it to look up a DMD pattern is done within a fraction of a second.

3.4 Test field 1: LG_{10} mode

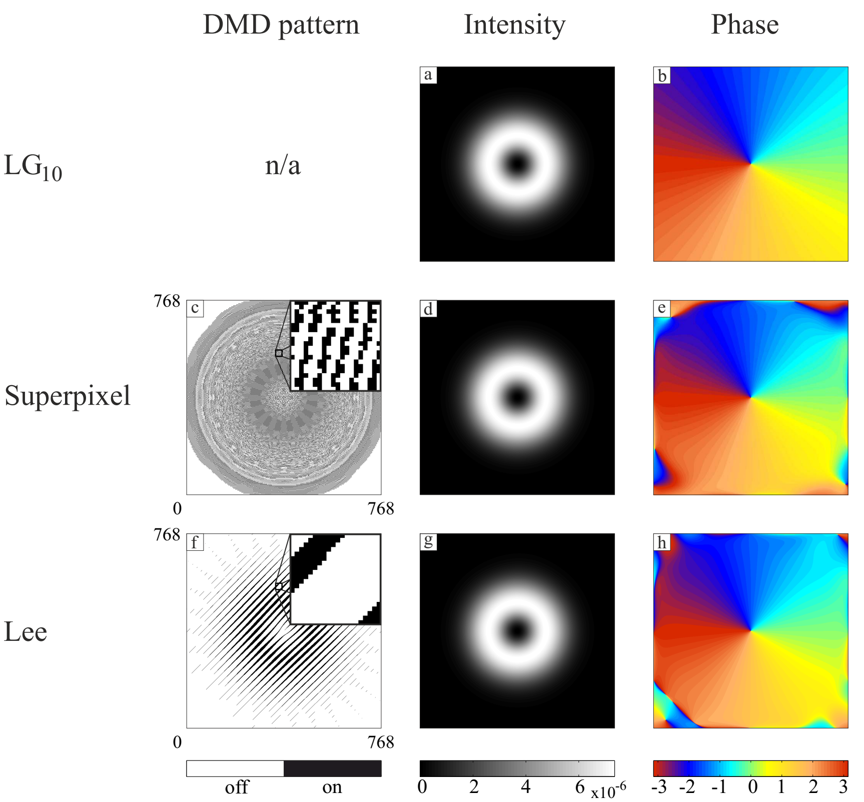


Figure 3.3: (a,b) Intensity and phase of the target LG_{10} mode. (c) DMD pattern for the LG_{10} mode when using the superpixel method. Inset: zoom-in on 20 × 20 DMD pixels. (d,e) Calculated intensity and phase using the superpixel method; $\delta_{\text{superpixel}} = 7 \cdot 10^{-5}$. (f) DMD pattern for the LG_{10} mode when using Lee holography with $k_x = k_y = \frac{2\pi}{30}$ pixel^{-1}. Inset: zoom-in on 20 × 20 DMD pixels. (g,h) Calculated intensity and phase using Lee holography; $\delta_{\text{Lee}} = 9 \cdot 10^{-5}$. Intensities are normalized to total intensity.

In order to test our method two test fields are constructed using superpixels of size $n = 4$. The first test field is a LG_{10} 'donut' mode with an orbital angular momentum of $l = 1$, where l is the azimuthal mode number. These modes have many applications [38], including micromanipulation [39, 40], imaging [41] and communication [6]. The intensity and phase profiles of such a mode are shown in Figs. 5.3(a) and 5.3(b). In order to apply our superpixel method, we normalize the amplitude of the LG_{10} mode to the maximum amplitude our method can create. For each superpixel we determine the pixel values using the lookup table. The resulting pattern on the DMD is shown in Fig. 5.3(c). For this low-resolution target field we tune the size r of the spatial filter such that $\Delta k' = \frac{\pi}{100}$ rad·pixel^{-1}. This corresponds to a feature size of approximately 100×100 DMD pixels and for our system this means $r = 0.07$ mm. From the DMD pattern we calculate the resulting target field by first applying a fast Fourier transform for the first lens, then a multiplication with a circular mask for the spatial filter and finally a second fast Fourier transform for the second lens. The intensity and phase profiles of the obtained field are shown in Figs. 5.3(d) and 5.3(e). We observe an excellent match, apart from the phase in the corners which is not well defined as the intensity of the ideal LG_{10} mode is negligible there. The fidelity of the superpixel method for this target field is calculated to be $F_{\text{superpixel}} = 0.99993$. In other words, a fraction of only $\delta_{\text{superpixel}} = 7 \cdot 10^{-5}$ of the light goes to other modes.

The present reference method is Lee holography [31]. Lee holography has two parameters: the size of the spatial filter and the spatial carrier frequency $\mathbf{k}$. The size of the spatial filter and therefore the system resolution are kept the same as when using the superpixel method. $\mathbf{k}$ is optimized to obtain maximum fidelity. The best result, which is obtained using $k_x = k_y = \frac{2\pi}{30}$ pixel^{-1}, is shown in Figs. 5.3(f)–5.3(h). Using this method the error $\delta_{\text{Lee}} = 9 \cdot 10^{-5}$. Both methods allow generation of a LG_{10} mode with very high fidelity using a DMD of standard size. The superpixel method is most accurate, offering a 18% reduction of error compared to Lee holography.

3.5 Test field 2: Image quality

Next, we consider a high resolution target field with uncorrelated intensity and phase. We choose a field which contains the picture of a dog in the intensity and a picture of a cat in the phase of the field, as shown in Figs. 3.4(a) and 3.4(b). Holographic methods are often used to project images and fully independent control over phase and amplitude of light is desired in many applications such as phase contrast microscopy [4]. Moreover, using this test field we show that the superpixel method can obtain a high resolution. We use superpixels of size $n = 4$ and in order to allow for a high resolution we use an aperture size $r = 0.9$ mm, which means the minimum feature size is 2×2 superpixels. Any imaging system, and therefore any modulation method, has a finite resolution due to apertures in the system and the finite extent of the optics. This finite resolution leads to inevitable correlations between amplitude and phase of light fields. In particular, it is impossible to make very large phase gradients without the amplitude becoming zero. For the current test field and resolution, the theoretical maximum

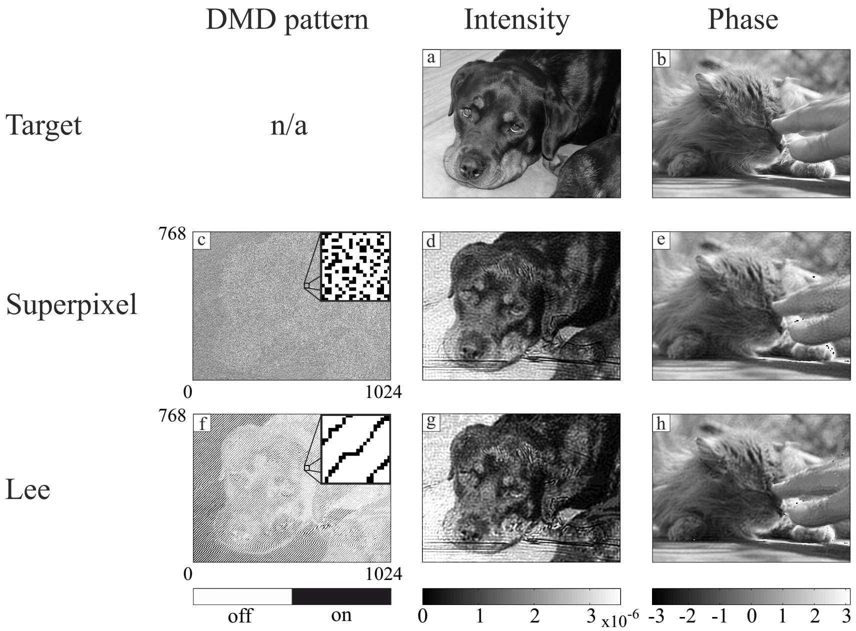


Figure 3.4: (a,b) Intensity and phase of a high resolution target field. (c) DMD pattern according to the superpixel method. Inset: zoom-in on 20 × 20 DMD pixels. (d,e) Calculated intensity and phase using the superpixel method; $\delta^{\Delta \mathrm{k}}_{\mathrm{superpixel}} = 0.8\%$. (f) DMD pattern according to the Lee method using $k_x = k_y = \frac{2\pi}{12}$ pixel^{-1}. Inset: zoom-in on 20 × 20 DMD pixels. (g,h) Calculated intensity and phase using the Lee method; $\delta^{\Delta \mathrm{k}}_{\mathrm{Lee}} = 1.6\%$. Intensities are normalized to total intensity.

fidelity that can be achieved is given by $F^{\Delta \mathrm{k}}_{\mathrm{theoretical}} = \left| E^{*}_{\mathrm{target}} E^{\Delta \mathrm{k}}_{\mathrm{target}} \right|^2 = 0.955$, where $E^{\Delta \mathrm{k}}_{\mathrm{target}}$ is the spatial bandwidth limited target field.

The DMD pattern and corresponding intensity and phase profiles that are obtained when using the superpixel method are shown in Figs. 3.4(c)–3.4(e). We optimize Lee holography and find the optimum for $k_x = k_y = \frac{2\pi}{12}$ pixel^{-1}. The resulting DMD pattern and obtained intensity and phase patterns are shown in Figs. 3.4(f)–3.4(h). In both cases we observe some undesired ripples in the obtained intensity profile, because the steepest phase gradients in the target field cannot be resolved by the 8 DMD pixel resolution of the superpixel and Lee methods. We observe that the reconstructed intensity is more accurate when using the superpixel method. For the superpixel method we find a fidelity of $F_{\mathrm{superpixel}} = 0.947 = 0.992 F^{\Delta \mathrm{k}}_{\mathrm{theoretical}}$, showing that the fidelity is almost the theoretical maximum for the 8 pixel resolution. The error with respect to the bandwidth limited target is $\delta^{\Delta \mathrm{k}}_{\mathrm{superpixel}} = 0.8\%$. For Lee holography we find $\delta^{\Delta \mathrm{k}}_{\mathrm{Lee}} = 1.6\%$. The superpixel method offers a large improvement, reducing the error by

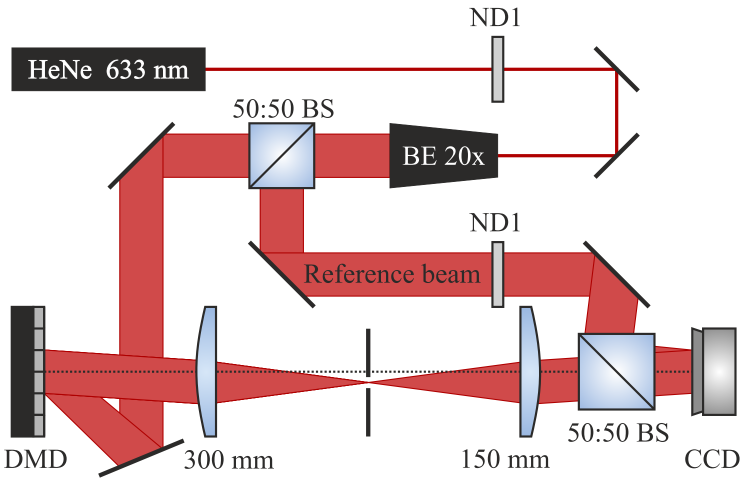


Figure 3.5: Experimental setup. DMD: ViALUX V4100, XGA resolution; CCD: AVT Dolphin F145-B; lenses: 2 inch achromats.

50% compared to Lee holography.

We experimentally verified the fidelity of our superpixel method using the experimental setup shown in Fig. 3.5 in combination with our publicly availabe control program implementing the superpixel method [37]. The constructed field is measured in the target plane on an AVT Dolphin F-145B CCD camera using off-axis digital holography [42]. The measured intensity is divided by the illumination intensity and from the measured phase we subtract the reference phase which is measured by constructing a plane wave. The measured field is shown in Fig. 3.6, along with the calculated field for comparison. We see that the measured field is almost identical to the calculated field. The fidelity of the measured field is $F_{\text{superpixel,measured}} = 0.94 = 0.98 F^{\Delta\text{k}}_{\text{theoretical}}$, providing experimental proof that the superpixel method accurately constructs complex high resolution light fields. The small difference between the measured and calculated fidelity seems to be due to air flow causing a small phase error.

3.6 Origin of residual errors

We identify two factors limiting the fidelity of the superpixel method. The first is the discrete approximation of the continuous target phases and amplitudes. In Fig. 5.2 we observe that for the case of superpixels of size 4×4 each superpixel can create a large variety of complex fields. However, as in any modulation method, the modulation is discrete and there is a discretisation error. For test field 2 we compare the target field at each superpixel to the field that would ideally be obtained according to Fig. 5.2. We define $F_{\text{discretisation}} = \left|E^{*}_{\text{target}} E_{\text{idealsuperpixels}}\right|^2$, where $E_{\text{idealsuperpixels}}$ are the fields that can ideally be created at the superpixels and are taken directly from Fig. 5.2(b). We find $F_{\text{discretisation}} = 0.9995$, which

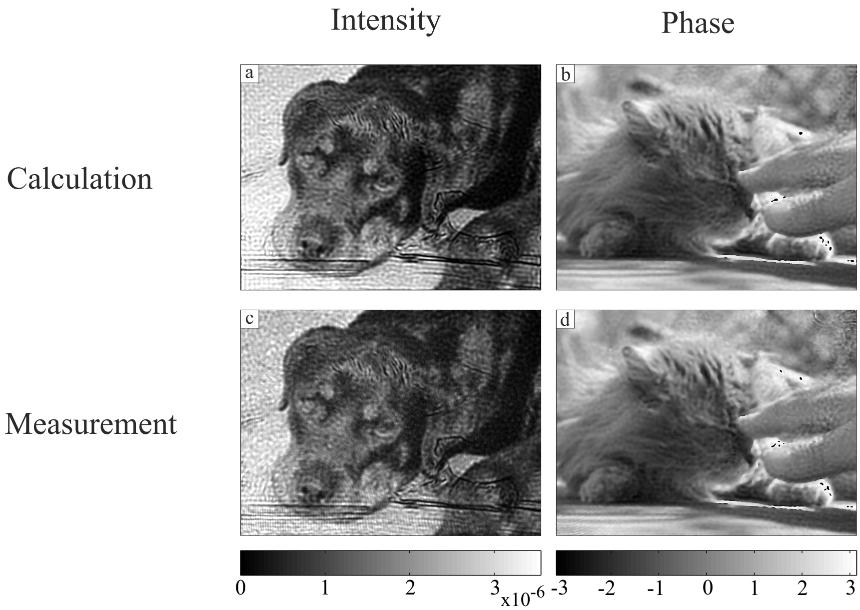


Figure 3.6: (a,b) Calculated intensity and phase using the superpixel method; $F_{\text{superpixel}} = 0.99F^{\Delta k}_{\text{theoretical}}$. (c,d) Measured intensity and phase using the superpixel method; $F_{\text{superpixel,measured}} = 0.98F^{\Delta k}_{\text{theoretical}}$. Intensities are normalized to total intensity.

means the discretisation error is an order of magnitude smaller than the total error.

The remaining error can be explained by the displacement of pixels with respect to the center of the superpixel. In the calculation of the fields that can be constructed by a superpixel, as displayed in Fig. 5.2, pixel responses are assumed to be Airy disks located exactly at the center of the superpixel. Our assumption that the field constructed by a superpixel is an Airy disk positioned at the center of the superpixel only holds in that approximation. The effect of pixel displacement on fidelity depends on spatial correlations in the target field. For a field that is spatially uncorrelated at the scale of the system resolution, such as a speckle field with a speckle grain size of 2×2 superpixels, the superpixel method achieves a fidelity $F = 0.97$, as compared to $F = 0.99$ for the more correlated test field 2. Resolution can be traded for fidelity: if the size of the spatial filter is reduced the resolution is reduced in exchange for a smaller relative pixel displacement and higher fidelity. For test field 1 we reach $F > 0.9999$ at a resolution of 100×100 DMD pixels.

Further reduction of the residual error may be possible by changing the position of the aperture in order to lift remaining degeneracy in the constructed fields, by taking into account the displacement error of the pixels when constructing the lookup table or by finding the optimal DMD setting iteratively to compensate for displacement errors. The simplicity of the current method is, however, a great advantage and may enable implementation in hardware such as Field Programmable Gate Arrays (FPGA).

3.7 Conclusions

We have demonstrated a superpixel based method to independently and accurately modulate the intensity and phase of light. Our method only requires very basic optics consisting of two lenses and a circular aperture, is very easy to align and highly robust to misalignment. The calculated modulation fidelity of our superpixel method exceeds 0.9999 for an LG_{10} mode, using 768×768 DMD pixels. Fidelity can be traded for resolution. We calculated and measured that at a resolution of 8×8 DMD pixels per diffraction limited spot the modulation fidelity is in the order of 0.99 for our test image with uncorrelated intensity and phase. The superpixel method offers a modulation fidelity exceeding that of current methods and is expected to benefit the areas of imaging, holography, optical communication and optical micromanipulation.

Bibliography

[1] M. Woerdemann, C. Alpmann, M. Esseling, and C. Denz, *Advanced optical trapping by complex beam shaping*, Laser Photon. Rev. **7**, 839 (2013). — p.31.

[2] C. Maurer, A. Jesacher, S. Bernet, and M. Ritsch-Marte, *What spatial light modulators can do for optical microscopy*, Laser Photon. Rev. **5**, 81 (2011). — p.31.

[3] B. Bhaduri, C. Edwards, H. Pham, R. Zhou, T. H. Nguyen, L. L. Goddard, and G. Popescu, *Diffraction phase microscopy: principles and applications in materials and life sciences*, Adv. Opt. Photon. **6**, 57 (2014). — p.31.

[4] A. B. Parthasarathy, K. K. Chu, T. N. Ford, and J. Mertz, *Quantitative phase imaging using a partitioned detection aperture*, Opt. Lett. **37**, 4062 (2012). — p.31, 37.

[5] L. Waller, G. Situ, and J. W. Fleischer, *Phase-space measurement and coherence synthesis of optical beams*, Nature Photon. **6**, 474 (2012). — p.31.

[6] G. Gibson, J. Courtial, M. J. Padgett, M. Vasnetsov, V. Pas'ko, S. M. Barnett, and S. Franke-Arnold, *Free-space information transfer using light beams carrying orbital angular momentum*, Opt. Express **12**, 5448 (2004). — p.31, 37.

[7] A. P. Mosk, A. Lagendijk, G. Lerosey, and M. Fink, *Controlling waves in space and time for imaging and focusing in complex media*, Nature Photon. **6**, 283 (2012). — p.31.

[8] I. M. Vellekoop and A. P. Mosk, *Focusing coherent light through opaque strongly scattering media*, Opt. Lett. **32**, 2309 (2007). — p.31, 32.

[9] E. G. van Putten, D. Akbulut, J. Bertolotti, W. L. Vos, A. Lagendijk, and A. P. Mosk, *Scattering lens resolves sub-100 nm structures with visible light*, Phys. Rev. Lett. **106**, 193905 (2011). — p.31.

[10] I. M. Vellekoop, E. G. van Putten, A. Lagendijk, and A. P. Mosk, *Demixing light paths inside disordered metamaterials*, Opt. Express **16**, 67 (2008). — p.31.
[11] C. L. Hsieh, Y. Pu, R. Grange, and D. Psaltis, *Digital phase conjugation of second harmonic radiation emitted by nanoparticles in turbid media*, Opt. Express **18**, 12283 (2010). — p.31.
[12] X. Xu, H. Liu, and L. V. Wang, *Time-reversed ultrasonically encoded optical focusing into scattering media*, Nature Photon. **5**, 154 (2011). — p.31.
[13] Y. M. Wang, B. Judkewitz, C. A. DiMarzio, and C. Yang, *Deep-tissue focal fluorescence imaging with digitally time-reversed ultrasound-encoded light*, Nat. Commun. **3**, 928 (2012). — p.31.
[14] K. Si, R. Fiolka, and M. Cui, *Fluorescence imaging beyond the ballistic regime by ultrasound-pulse-guided digital phase conjugation*, Nature Photon. **6**, 657 (2012). — p.31.
[15] J. Aulbach, B. Gjonaj, P. M. Johnson, A. P. Mosk, and A. Lagendijk, *Control of light transmission through opaque scattering media in space and time*, Phys. Rev. Lett. **106**, 103901:1 (2011). — p.31.
[16] O. Katz, E. Small, Y. Bromberg, and Y. Silberberg, *Focusing and compression of ultrashort pulses through scattering media*, Nature Photon. **5**, 372 (2011). — p.31.
[17] D. J. McCabe, A. Tajalli, D. R. Austin, P. Bondareff, I. A. Walmsley, S. Gigan, and B. Chatel, *Spatio-temporal focusing of an ultrafast pulse through a multiply scattering medium*, Nat. Commun. **2**, 447 (2011). — p.31.
[18] J. H. Park, C. Park, H. Yu, Y. H. Cho, and Y. Park, *Dynamic active wave plate using random nanoparticles*, Opt. Express **20**, 17010 (2012). — p.32.
[19] Y. F. Guan, O. Katz, E. Small, J. Y. Zhou, and Y. Silberberg, *Polarization control of multiply scattered light through random media by wavefront shaping*, Opt. Lett. **37**, 4663 (2012). — p.32.
[20] J. H. Park, C. Park, H. Yu, and Y. Cho, Y. H. Park, *Active spectral filtering through turbid media*, Opt. Lett. **37**, 3261 (2012). — p.32.
[21] E. Small, O. Katz, Y. F. Guan, and Y. Silberberg, *Spectral control of broadband light through random media by wavefront shaping*, Opt. Lett. **37**, 3429 (2012). — p.32.
[22] S. R. Huisman, T. J. Huisman, S. A. Goorden, A. P. Mosk, and P. W. H. Pinkse, *Programming balanced optical beam splitters in white paint*, Opt. Express **22**, 8320 (2014). — p.32.
[23] D. Dudley, W. M. Duncan, and J. Slaughter, *Emerging digital micromirror device (DMD) applications*, Proc. SPIE **4985**, 14 (2003). — p.32.
[24] D. Akbulut, T. J. Huisman, E. G. van Putten, W. L. Vos, and A. P. Mosk, *Focusing light through random photonic media by binary amplitude modulation*, Opt. Express **19**, 4017 (2011). — p.32.
[25] B. R. Brown and A. W. Lohmann, *Computer-generated binary holograms*, IBM J. Res. Develop. **13**, 160 (1969). — p.32.
[26] T. Kreis, P. Aswendt, and R. Höfling, *Hologram reconstruction using a digital micromirror device*, Opt. Eng. **40**, 926 (2001). — p.32.
[27] E. Ulusoy, L. Onural, and H. M. Ozaktas, *Synthesis of three-dimensional*

light fields with spatial light modulators, J. Opt. Soc. Am. A **28**, 1211 (2011). — p.32.

[28] W.-H. Lee, in *Computer-generated holograms: Techniques and applications*, Vol. 16 of *Progress in Optics*, edited by E. Wolf (Elsevier, 1978), pp. 119 – 232. — p.32.

[29] G. Tricoles, *Computer generated holograms: an historical review*, Appl. Opt. **26**, 4351 (1987). — p.32.

[30] G. Nehmetallah and P. P. Banerjee, *Applications of digital and analog holography in three-dimensional imaging*, Adv. Opt. Photon. **4**, 472 (2012). — p.32.

[31] W.-H. Lee, *Binary synthetic holograms*, Appl. Opt. **13**, 1677 (1974). — p.32, 37.

[32] D. B. Conkey, A. M. Caravaca-Aguirre, and R. Piestun, *High-speed scattering medium characterization with application to focusing light through turbid media*, Opt. Express **20**, 1733 (2012). — p.32.

[33] M. Mirhosseini, O. S. Magaña Loaiza, C. Chen, B. Rodenburg, M. Malik, and R. W. Boyd, *Rapid generation of light beams carrying orbital angular momentum*, Opt. Express **21**, 30196 (2013). — p.32.

[34] V. Lerner, D. Shwa, Y. Drori, and N. Katz, *Shaping Laguerre-Gaussian laser modes with binary gratings using a digital micromirror device*, Opt. Lett. **37**, 4826 (2012). — p.32.

[35] E. Ulusoy, L. Onural, and H. M. Ozaktas, *Full-complex amplitude modulation with binary spatial light modulators*, J. Opt. Soc. Am. A **28**, 2310 (2011). — p.32.

[36] E. G. van Putten, I. M. Vellekoop, and A. P. Mosk, *Spatial amplitude and phase modulation using commercial twisted nematic LCDs*, Appl. Opt. **47**, 2076 (2008). — p.32, 33, 34.

[37] S. A. Goorden, J. Bertolotti, and A. P. Mosk, *Control software for superpixel-based phase and amplitude modulation using a DMD, open source: https://sourceforge.net/projects/fullfieldmodulation/files/*, 2014. — p.35, 39.

[38] A. M. Yao and M. J. Padgett, *Orbital angular momentum: origins, behavior and applications*, Adv. Opt. Photon. **3**, 161 (2011). — p.37.

[39] T. Puppe, I. Schuster, A. Grothe, A. Kubanek, K. Murr, P. W. H. Pinkse, and G. Rempe, *Trapping and observing single atoms in a blue-detuned intracavity dipole trap*, Phys. Rev. Lett. **99**, 013002 (2007). — p.37.

[40] L. Allen, M. W. Bijersbergen, R. J. C. Spreeuw, and J. P. Woerdman, *Orbital angular momentum of light and the transformation of laguerre-gaussian laser modes*, Phys. Rev. A **45**, 8185 (1992). — p.37.

[41] S. W. Hell and J. Wichmann, *Breaking the diffraction resolution limit by stimulated emission: stimulated-emission-depletion fluorescence microscopy*, Opt. Lett. **19**, 780 (1994). — p.37.

[42] M. Takeda, H. Ina, and S. Kobayashi, *Fourier-transform method of fringe-pattern analysis for computer-based topography and interferometry*, J. Opt. Soc. Am. **72**, 156 (1982). — p.39.

CHAPTER 4

Apparatus for full access to modes in disordered media

In this chapter we describe an apparatus with which we aim at an unparalleled degree of control over light in photonic structures. Our goal is to elucidate phenomena such as open transmission channels and long-lived modes in strongly scattering samples. The apparatus is designed to perform digital optical phase conjugation on both sides of the sample as well as transmission matrix measurements with high fidelity. A frequency-tunable laser is employed to investigate modes in the frequency domain.

4.1 Introduction

Full control over the scattering matrix of a multiple-scattering medium is useful in a wide range of fields. It enables experimental investigation of properties of random scattering materials, such as the existence of open channels and long-lived modes, as described in Chapter 2. Exploring and manipulating such channels and modes is of fundamental interest and may have applications in e.g. LEDs and solar cells [1]. An apparatus that fully controls light scattering could also be an excellent tool for imaging underneath the skin, as well as for high-resolution imaging using a high-index scattering lens [2]. Other fields with high societal relevance in which light scattering is increasingly important are the fields of optical communication and of security. Security in authentication can be enhanced using methods such as Quantum-Secure Authentication (Chapter 5), whereas security in message encryption can be enhanced using methods such as Quantum Key Distribution [3]. Both rely on or can benefit from full control over light scattering.

To enable a high level of control over light scattering we constructed an apparatus that can measure and synthesize the light field on both sides of a slab-geometry sample. The geometry of the apparatus is shown in Fig. 4.1. The sample module is at the center of the apparatus. Combinations of vector field synthesizer and detector modules allow control over the light field at both sides of the sample. Light is transported from the light source module to the synthesizer modules through optical fibers. The light is shaped and travels to the

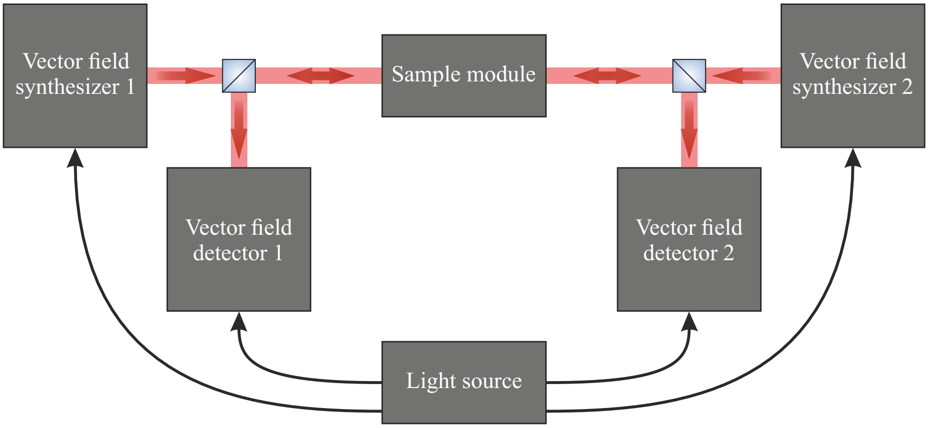


Figure 4.1: Schematic of the apparatus. Modules (grey boxes) are connected through fibers (black arrows) or free space propagation (red bars).

sample module. After interaction with the sample, the reflected as well as the transmitted light travels to the detection modules, where it is recombined with reference beams that come directly from the light source module.

The primary goal of the apparatus is to investigate open channels and long-lived modes of multiple-scattering samples. From this goal, we derive a number of requirements that the apparatus must fulfill. The requirements follow from a few useful scaling laws describing propagation of light through multiple-scattering media. The average transmission scales as l_{tr}/L, where l_{tr} is the transport mean free path [4] and L is the sample thickness. For $L/l_{\mathrm{tr}} > 10$ the average transmission falls below approximately 0.1, so that the transmission of open channels with order unity transmission is clearly higher than the average. The characteristic lifetime of optical modes in the diffusive regime is the Thouless time $\tau_{\mathrm{Th}} = L^2/D$, where the diffusion constant $D = \frac{1}{3} v_{\mathrm{E}} l_{\mathrm{tr}}$ and v_{E} is the transport velocity [5]. Although not much is known about the distribution of long-lived modes for light, it is to be expected that the sample should be in the multiple-scattering regime, i.e. $L/l_{\mathrm{tr}} > 10$. The lateral spatial extent of channels is roughly $(2L)^2$ as estimated from diffusion theory. The number of effective pixels required to address channels is rougly equal to the number of speckle spots covered by the channel: $(2L)^2/(\lambda/(2n))^2$, where λ is the wavelength and n is the refractive index of the substrate. It is advantageous to keep this number low to reduce complexity. For samples with thicknesses up to $L = 15\,\mu$m the required number of pixels is limited to approximately 10^4. For the field synthesizers and detectors we define fidelities as $F = |E^*_{\mathrm{ideal}} E_{\mathrm{experimental}}|^2$, where E_{ideal} and $E_{\mathrm{experimental}}$ are the ideal and the experimentally obtained light fields and both fields are normalized to their total power. We obtain the following list of requirements:

Sample requirements

1. Thickness $L > 10 l_{\mathrm{tr}}$ so that the sample is deep in the multiple scattering regime, $L < 15\,\mu\mathrm{m}$ so that the transmitted light falls within the field of view of the optics

2. Transport mean free path $l_{\mathrm{tr}} < 1\,\mu\mathrm{m}$ so that requirement 1 can be fulfilled

3. Homogeneous on a $10\,\mu\mathrm{m}$ scale (e.g. no holes)

4. No strong surface reflections

5. Stable for $> 10\,\mathrm{s}$

Optical access to the sample

1. Field of view $> 25\,\mu\mathrm{m}$

2. NA> 0.9 to collect $> 80\%$ of the light

Light source requirements

1. Tuning range $> \lambda/100$ to resolve modes with average lifetime

2. Tuning resolution $< \lambda/10^4$ to resolve modes with long lifetime

Field synthesizer requirements

1. Resolution $> 100 \times 100$ effective pixels

2. Modulation fidelity $F > 0.9$ (this implies that phase, amplitude and polarization must be modulated)

Field detector requirements

1. Resolution $> 100 \times 100$ effective pixels

2. Detection fidelity of $F > 0.95$ (this implies that phase, amplitude and polarization must be detected)

A box around the apparatus isolates the apparatus from the environment. The first effect of this is that it suppresses air turbulence, which otherwise causes fluctuations in the transmitted wavefronts. The second effect of the box is that it eliminates background light.

A detailed description of the various modules in the apparatus is provided in the rest of this chapter. The light source is described in Section 4.2, the vector field synthesis in Section 4.3, the sample in Section 4.4 and the vector field detection in Section 4.5. Finally, the alignment procedure for the vector field synthesis and detection modules is described in Section 4.6.

4.2 Light source module

The basis of the light source module is formed by the New Focus Velocity TLB-6712 tunable diode laser. A schematic of the laser is shown in Fig. 4.2.

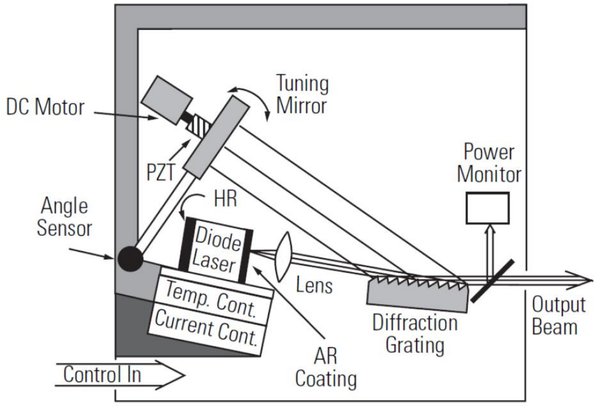


Figure 4.2: Schematic of the New Focus Velocity TLB-6712 tunable diode laser head. The laser uses a Littman-Metcalf configuration, in which the movement path of the tuning mirror with respect to the diffraction grating is carefully designed to ensure mode-hop-free tuning. Image from [6].

The New Focus Velocity is an external cavity diode laser. The gain medium is a diode laser. The cavity is formed by a highly reflective coating on the laser diode and a tuning mirror which is mounted on a movable stiff arm. A diffraction grating is placed inside the cavity. Dispersion of this grating causes all light frequencies except one to diffract out of the cavity. The frequency that stays inside the cavity, i.e. the lasing frequency, can be selected by moving the tuning mirror. The mirror moves in such a way that the change in cavity length is precisely matched to the change in frequency, in a Littman-Metcalf configuration. Therefore, the laser keeps lasing in the same mode and is tuned mode-hop-free.

The scanning range is 765 - 781 nm. The base resolution is 0.01 nm, piezo fine tuning allows sub-picometer resolution [7]. The linewidth of around 1 MHz, integrated over 1 s, is several orders of magnitude narrower than the frequency-tuning resolution [8]. Even without the piezo fine tuning option, this laser allows us to investigate a range of pathlengths from around 40 μm up to 6 cm, or lifetimes of around 130 fs up to 0.2 ns.

The complete light source module is shown schematically in Fig. 4.3. The laser light passes through a Faraday isolator, preventing back reflection into the laser. The light beam is split into six beams by polarizing beam splitters. The relative intensities of the beams are tunable using zero-order half-wave plates. Each beam is coupled into a single-mode polarization-maintaining (SMPM) fiber through a fiber collimator with fine focussing mechanism (Schäfter+Kirchhoff), mounted in a high-precision and high-stability mirror mount (Liop-Tec). Coupling efficiencies

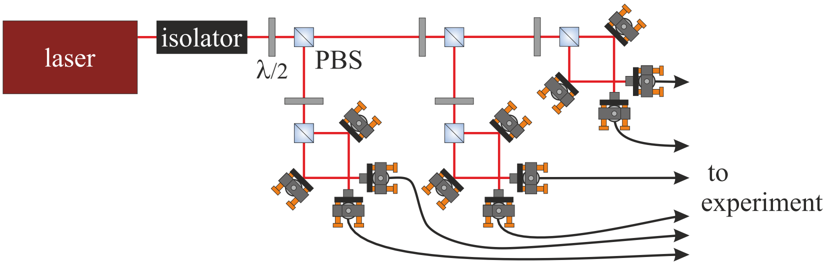


Figure 4.3: Schematic of the light source module. The laser beam is split into six beams, of which the relative intensities can be tuned by wave-plates. Each beam is coupled through a fiber collimator into a single-mode polarization-maintaining fiber.

are around 60%, limited by the elliptical beam profile of the laser. Transporting the light through the SMPM fibers ensures a stable and smooth near-Gaussian beam profile, with the additional benefit of enhanced flexibility: we can easily lead the fibers to where we need the light.

4.3 Vector field synthesis module

The Digital Micromirror Device (DMD) forms the core of the vector field synthesis module. The DMD is a Vialux V-9600 module containing a 0.96" WUXGA resolution DMD chip for visible light, produced by Texas Instruments. The chip contains 1920×1200 pixels at a 10.8 μm pitch. Each pixel consists of an aluminum mirror that can rotate around a diagonal axis to two defined positions, called the "on" and "off" states of the pixel. The chip can operate at a frame rate of 16393 fps. A SEM image of a similar DMD chip are shown in Fig. 4.4.

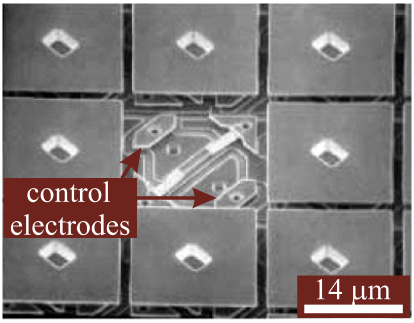


Figure 4.4: SEM image of a Texas Instruments XGA resolution DMD chip, consisting of 13.68 μm size aluminum mirrors. One mirror is missing to show the underlying structure. We recognize the two control electrodes, used to tilt the mirror to "on" and "off" positions. SEM image by Texas Instruments.

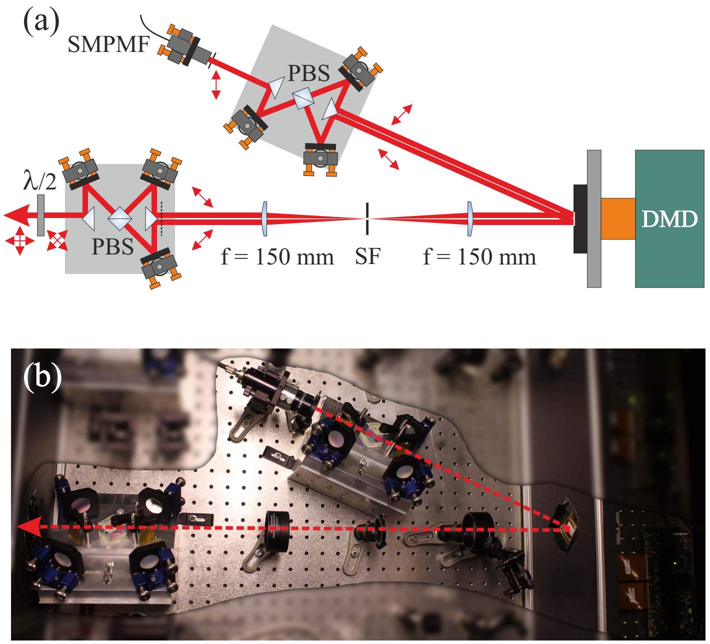


Figure 4.5: (a) Schematic of the vector field synthesis module. Light is coupled out of a single-mode polarization-maintaining fiber (SMPMF) into a collimated beam. The beam is split into two orthogonally polarized beams by a polarizing beamsplitter cube (PBS) under a 45° angle with respect to the table (not shown). After reflection from the digital micromirror device (DMD) the beams are Fourier filtered by a spatial filter (SF) and imaged to an intermediate image plane by two lenses in a 4f-configuration. The beams are recombined by a recombination device and the polarization is rotated by 45° by a half-wave plate. (b) Photograph of a vector field synthesis module. The red dashed line is a guide to the eye indicating the approximate beam paths.

Full control over phase, amplitude and polarization of light is obtained using additional optics. The complete vector field synthesis module is shown in Fig. 4.5. The DMD is rotated by 45° along the normal to the chip, so that the rotation axis of the micromirrors becomes vertical. This ensures that light beams remain in the horizontal plane after reflecting from the DMD. Laser light is coupled out of a single-mode polarization-maintaining fiber into a vertically polarized collimated beam with a diameter of 18 mm by a fiber collimator (Schäfter+Kirchhoff). The beam can be clipped to the desired size by an aperture, typically with a diameter of 5-10 mm. The beam is split into two orthogonally polarized beams. The beams propagate parallel to each other and are separated by approximately 1 cm in the diagonal direction so that they fall in the centers of the two halves of the DMD. The splitting device consists of a polarizing beam splitter, three folding mirrors and two gold-coated prisms to ensure the incident and outgoing Poynting vectors are parallel. These elements are placed on a solid aluminum block for stability. The block has an angle of 45^o to match the angle of the DMD, as shown in Fig. 4.5(b). The DMD plane is imaged to an intermediate image plane using two planoconvex 2" achromatic lenses with focal lengths of 150 mm. Both beams pass through a single circular spatial filter in the Fourier plane, allowing independent phase and amplitude modulation of each polarization component using either the superpixel method, as described in Chapter 3, or Lee holography. The two beams are recombined using a recombination device which is identical to the splitting device and performs the inverse operation. Finally, a half-wave plate rotates the polarization by 45^o. By doing so the vertical and horizontal polarization components of the target field are mapped to the left and right halves of the DMD, for convenient operation.

The vector field synthesis module provides full control over phase, amplitude and polarization of light using a single DMD. The modulation fidelity of each polarization component depends on the target field and is designed to be of the same high level as demonstrated in Chapter 3. An important aspect of achieving a high modulation fidelity is to compensate for the non-flatness of the DMD chip. This is done by imaging the DMD onto a field detector and subtracting the measured phase profile when synthesizing fields. Integration of the polarization splitting and recombination devices on solid aluminum blocks in combination with a design that features equal path lengths and parallel beams leads to very high phase stability between the polarization components. Crosstalk between polarizations is only limited by the extinction ratio of the polarizing beamsplitter cubes and designed to be below 0.1%.

4.4 Sample module

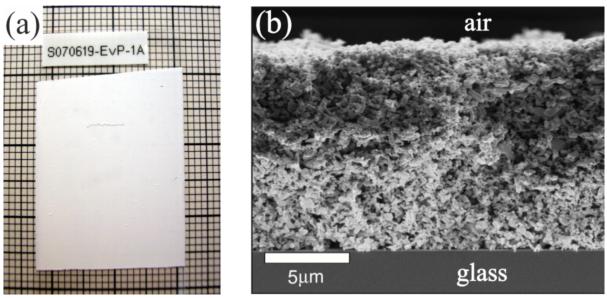


Figure 4.6: (a) Photograph of ZnO sample on a background of millimeter paper. The sample is seen to be fully opaque. (b) Scanning electron microscope image of a cross-section of a ZnO sample. The ZnO-air interface is seen at the top and the ZnO-glass interface at the bottom. Images from [9].

The central part of the sample module is the sample. In order to have maximum access to open channels and long-lived modes we use a sample that scatters strongly within a volume with a thickness below $L = 20\,\mu$m. Also important to be able to investigate and address modes is that the sample is stable during the timespan of a typical experiment, i.e. several seconds. A low effective refractive index is desirable to minimize interface effects. Finally, low absorption is required to prevent long-lived modes from being absorbed. Zinc oxide (ZnO) nanoparticles in air satisfy all our requirements. We use a sample, prepared by Elbert van Putten, which consists of commercially available ZnO nano powder with an average grain size of 200 nm (Aldrich Zinc Oxide, $< 1\mu$m 99.9%) spray painted onto a 160 μm thick microscope cover glass. The recipe is described in [10]. A photograph and a SEM image of a similar sample are shown in Fig. 4.6. Such samples have an effective refractive index of $n_{\text{eff}} = 1.4 \pm 0.06$ and a transport mean free path of $l_{\text{tr}} = 0.73 \pm 0.15\,\mu$m at a wavelength of 770 nm [10]. Our sample has a thickness $L = 12 \pm 2\,\mu$m, so that $L/l_{\text{tr}} = 17 \pm 5$. Speckle patterns transmitted through samples similar to ours are found to be stable for at least an hour [9].

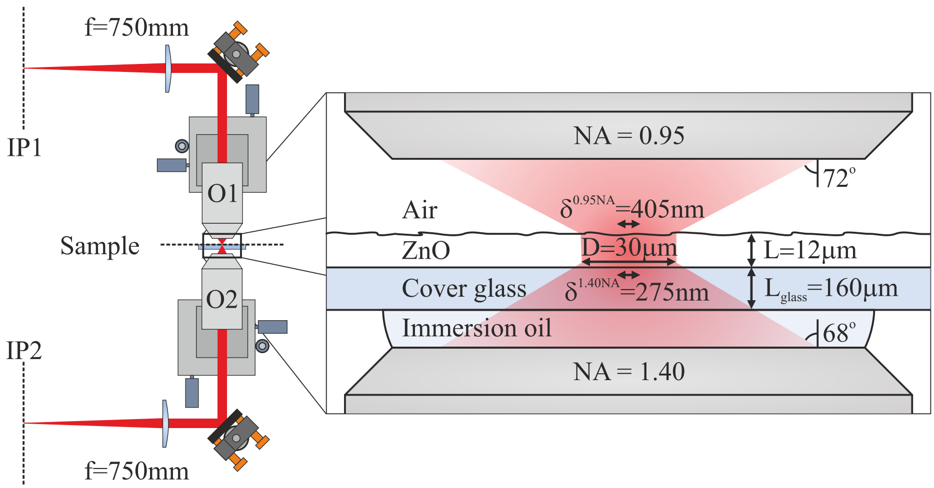


Figure 4.7: Schematic of the sample module. Image planes 1 and 2 (IP1 and IP2) are imaged to the sample surfaces using infinity corrected microscope objectives (O1 and O2) paired with tube lenses. Each objective is mounted on a manual 3D stage. The inset shows a zoom-in on the sample area. A $L = 12\,\mu$m thick ZnO layer on a $L_{\text{glass}} = 160\,\mu$m thick cover glass is accessed by a 0.95 NA air objective from the air side and a 1.40 NA oil immersion objective from the glass side. A region of the sample with a diameter $D = 30\,\mu$m is controlled with a diffraction limited spot size of $\delta^{0.95\text{NA}} = 405$ nm on the air side and $\delta^{1.40\text{NA}} = 275$ nm on the glass side.

The sample is part of the sample module, which is shown schematically in Fig. 4.7. A first image plane (IP1) is imaged to the sample surface using a tube lens (2" achromat) with focal length $f = 750$ mm and a 0.95 NA 63x magnification air objective (Zeiss Achroplan, O1). The opposite sample surface is imaged to another image plane (IP2) using a 1.40 NA 63x oil immersion objective (Zeiss Plan-Apochromat, O2) and a tube lens (2" achromat) with focal length $f = 750\,\mathrm{mm}$. Both objectives are placed on manual 3D stages.

High-NA microscope objectives provide good optical access to the sample, as is schematically shown in the inset of Fig. 4.7. The 0.95 NA air objective at the ZnO-air interface has a diffraction limited spot size with a full width at half maximum (FWHM) of $\delta^{0.95\mathrm{NA}} = 405\,\mathrm{nm}$ at a wavelength $\lambda = 770\,\mathrm{nm}$. This imposes a hard limit on how accurately we can address speckle-like channels, given by $\|F^{0.95\mathrm{NA}}_{\mathrm{speckle}}\|^2 = \|E^*_{\mathrm{speckle}} E^{0.95\mathrm{NA}}_{\mathrm{speckle}}\|^2 = (\lambda/2)^2/(\delta^{0.95\mathrm{NA}})^2 = 0.90$, where E_{speckle} is the channel profile in air and $E^{0.95\mathrm{NA}}_{\mathrm{speckle}}$ is the channel profile Fourier filtered to match the NA of the objective. The 1.40 NA oil immersion objective at the ZnO-glass interface provides a diffraction limited spot size of $\delta^{1.40\mathrm{NA}} = 275\,\mathrm{nm}$. The limit on how accurately we can address modes from this side is $\|F^{1.40\mathrm{NA}}_{\mathrm{speckle}}\|^2 = (\lambda/2n_{\mathrm{glass}})^2/(\delta^{1.40\mathrm{NA}})^2 = 0.85$, where $n_{\mathrm{glass}} = 1.515$ is the refractive index of the immersion oil and the glass. The effective number of superpixels on the DMD, in the order of 10^4, allows control over roughly 100^2 diffraction limited spots. For symmetry, we choose to control an area with a diameter of up to $D = 30\,\mu\mathrm{m}$ on both sides of the sample, which is sufficiently larger than the typical spatial extent of a channel estimated as $2L = 24\,\mu\mathrm{m}$.

The calculated magnification on both sides of the sample is 286x. This results in speckle sizes of $116\,\mu\mathrm{m}$ and $79\,\mu\mathrm{m}$ in IP1 and IP2, respectively. These can be resolved by our vector field synthesizers, which have an effective resolution of approximately $80\,\mu\mathrm{m}$ for superpixels of size 4×4.

4.5 Vector field detection module

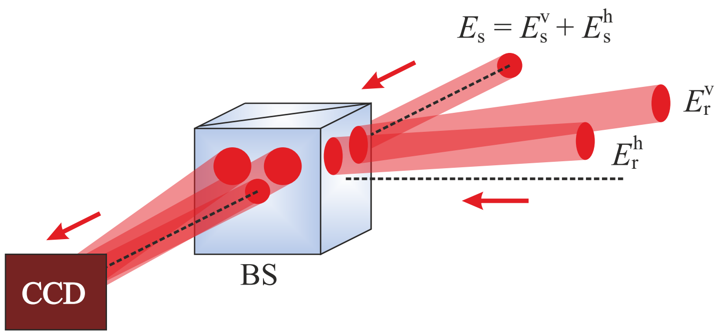


Figure 4.8: Schematic of the vector field detection module. The signal beam E_s illuminates the detector (CCD) along the normal. On the detector E_s interferes with two plane wave reference beams E_r^v and E_r^h, which illumate the detector under angles of approximately 1° with respect to the normal.

The function of the vector field detection module is to measure the spatial phase, amplitude and polarization distribution of a light field. Since the temporal frequency of light in the optical regime is too high to have direct access to the phase of light, we have to resort to interferometric methods or to e.g. microlens-based or partioned aperture-based wavefront sensors [11]. We use off-axis holographic detection, because it allows accurate, single-shot, high-resolution, polarization-resolved field detection. Takeda proposed digital off-axis holography for field detection of a single polarization [12] and it has been widely used since then. Akbulut and co-workers improved the method to work with a reference beam with an unknown intensity profile and compensated for the modulation transfer function caused by pixelation of the detector [13]. We implement polarization-resolved digital off-axis holography, as described by Colomb and co-workers [14].

A schematic representation of the detection module is shown in Fig. 4.8. The detector is a monochromatic CCD camera with 1392×1040 pixels of $6.45\,\mu$m by $6.45\,\mu$m size (Dolphin F145-B). Two reference beams $E_{\rm r}^{\rm h}$ and $E_{\rm r}^{\rm v}$, with horizontal and vertical polarization, are coupled out of single-mode polarization-maintaining fibers by fiber collimators into collimated beams with a diameter of 10.9 mm. The reference beams are reflected from a 50:50 beam splitter (BS) and illuminate the detector under angles of around 1° with respect to the normal. The camera is illuminated diagonally, i.e. from the side as well as from the top (not shown). The signal beam $E_{\rm s}$ is transmitted through the 50:50 beamsplitter and illuminates the detector along its normal. On the camera the reference beams interfere with $E_{\rm s}^{\rm h}$ and $E_{\rm s}^{\rm v}$, the horizontal and vertical components of the signal beam, respectively.

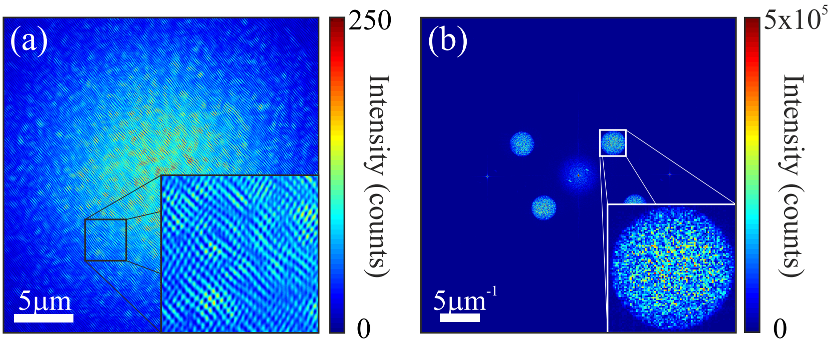


Figure 4.9: (a) Recorded interference pattern when the signal $E_{\rm s}$ is a speckle pattern. The inset shows a zoom-in on the fringes along both diagonal directions. (b) Modulus of the Fourier transform of the interference pattern shown in (a). The four interference terms are spatially separated from the central region. This allows us to isolate $\mathcal{F}\left\{E_{\rm s}^{\rm v}E_{\rm r}^{\rm v*}\right\}$ and $\mathcal{F}\left\{E_{\rm s}^{\rm h}E_{\rm r}^{\rm h*}\right\}$ from the other terms. The inset shows a zoom-in on $|\mathcal{F}\left\{E_{\rm s}^{\rm v}E_{\rm r}^{\rm v*}\right\}|$.

A typical interference pattern obtained when E_s is speckle is shown in Fig. 4.9(a). The inset shows fringes in both diagonal directions that correspond to interference between the signal and the two reference beams. The interference

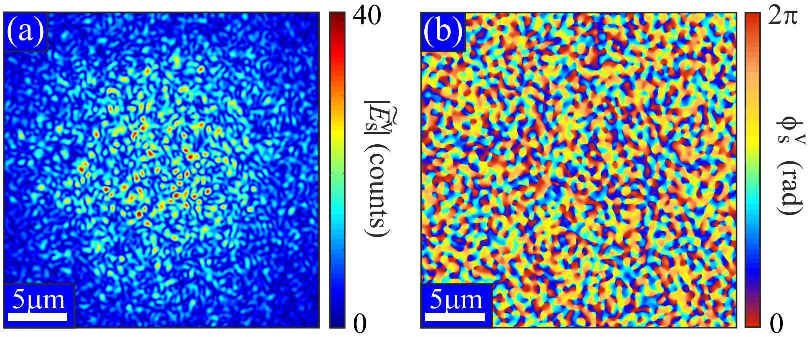


Figure 4.10: (a) Modulus and (b) phase of the vertical polarization component of the obtained $\widetilde{E}_{\mathrm{s}}$ at the surface of a $12\,\mu$m ZnO sample. The horizontal polarization component is similar and not shown.

pattern is described by

$$
\begin{aligned}
I = & \left(E_{\mathrm{s}}^{\mathrm{v}} + E_{\mathrm{s}}^{\mathrm{h}} + E_{\mathrm{r}}^{\mathrm{v}} + E_{\mathrm{r}}^{\mathrm{h}}\right)^{*} \; \left(E_{\mathrm{s}}^{\mathrm{v}} + E_{\mathrm{s}}^{\mathrm{h}} + E_{\mathrm{r}}^{\mathrm{v}} + E_{\mathrm{r}}^{\mathrm{h}}\right) && (4.1\mathrm{a})\\
= & |E_{\mathrm{s}}^{\mathrm{v}}|^2 + |E_{\mathrm{s}}^{\mathrm{h}}|^2 + |E_{\mathrm{r}}^{\mathrm{v}}|^2 + |E_{\mathrm{r}}^{\mathrm{h}}|^2 \\
& + E_{\mathrm{s}}^{\mathrm{v}*} E_{\mathrm{r}}^{\mathrm{v}} + E_{\mathrm{s}}^{\mathrm{h}*} E_{\mathrm{r}}^{\mathrm{h}} + E_{\mathrm{s}}^{\mathrm{v}} E_{\mathrm{r}}^{\mathrm{v}*} + E_{\mathrm{s}}^{\mathrm{h}} E_{\mathrm{r}}^{\mathrm{h}*}, && (4.1\mathrm{b})
\end{aligned}
$$

where position dependence of all terms is omitted for clarity. The signal beam has amplitude and phase defined as

$$
\begin{aligned}
E_{\mathrm{s}}^{\mathrm{v}}(x,y) = & |E_{\mathrm{s}}^{\mathrm{v}}(x,y)| e^{i\phi_{\mathrm{s}}^{\mathrm{v}}(x,y)}, \\
E_{\mathrm{s}}^{\mathrm{h}}(x,y) = & |E_{\mathrm{s}}^{\mathrm{h}}(x,y)| e^{i\phi_{\mathrm{s}}^{\mathrm{h}}(x,y)}.
\end{aligned}
$$

The reference beams enter at different angles so that their phase varies across the camera sensor according to

$$
\begin{aligned}
E_{\mathrm{r}}^{\mathrm{v}}(x,y) = & |E_{\mathrm{r}}^{\mathrm{v}}(x,y)| e^{-i2\pi(p_{\mathrm{x}}x + p_{\mathrm{y}}y)}, \\
E_{\mathrm{r}}^{\mathrm{h}}(x,y) = & |E_{\mathrm{r}}^{\mathrm{h}}(x,y)| e^{-i2\pi(q_{\mathrm{x}}x + q_{\mathrm{y}}y)},
\end{aligned}
$$

with $(p_{\mathrm{x}}, p_{\mathrm{y}})$ and $(q_{\mathrm{x}}, q_{\mathrm{y}})$ the carrier frequencies of the vertically and horizontally polarized plane wave reference beams. We take the Fourier transform of expression 4.1b and obtain

$$
\begin{aligned}
\mathcal{F}(I) = & \mathcal{F}\left\{|E_{\mathrm{s}}^{\mathrm{v}}|^2 + |E_{\mathrm{s}}^{\mathrm{h}}|^2 + |E_{\mathrm{r}}^{\mathrm{v}}|^2 + |E_{\mathrm{r}}^{\mathrm{h}}|^2\right\} \\
& + \mathcal{F}\left\{E_{\mathrm{s}}^{\mathrm{v}*} E_{\mathrm{r}}^{\mathrm{v}}\right\} + \mathcal{F}\left\{E_{\mathrm{s}}^{\mathrm{h}*} E_{\mathrm{r}}^{\mathrm{h}}\right\} + \mathcal{F}\left\{E_{\mathrm{s}}^{\mathrm{v}} E_{\mathrm{r}}^{\mathrm{v}*}\right\} + \mathcal{F}\left\{E_{\mathrm{s}}^{\mathrm{h}} E_{\mathrm{r}}^{\mathrm{h}*}\right\}. \quad (4.4)
\end{aligned}
$$

The five terms in expression 4.4 are spatially separated when the carrier frequencies $(p_{\mathrm{x}}, p_{\mathrm{y}})$ and $(q_{\mathrm{x}}, q_{\mathrm{y}})$ are chosen larger than the spatial bandlimit of E_{s}.

An example is shown in Fig. 4.9(b). The region in the middle, which is centered at $(k_x, k_y) = (0, 0)$, contains the sum of the reference and signal intensities in momentum space. The surrounding regions contain the interference terms: $\mathcal{F}\left\{E_s^{v*}E_r^{v}\right\}$ and $\mathcal{F}\left\{E_s^{v}E_r^{v*}\right\}$ centered at $(k_x, k_y) = \pm(p_x, p_y)$ and $\mathcal{F}\left\{E_s^{h*}E_r^{h}\right\}$ and $\mathcal{F}\left\{E_s^{h}E_r^{h*}\right\}$ centered at $(k_x, k_y) = \pm(q_x, q_y)$. We now isolate $\mathcal{F}\left\{E_s^{v}E_r^{v*}\right\}$, translate it to $(k_x, k_y) = (0, 0)$ to eliminate the phase gradient induced by the reference carrier frequency and apply the inverse Fourier transform to obtain

$$\widetilde{E}_s^{v}(x, y) = |E_s^{v}(x, y)E_r^{v}(x, y)|e^{i\phi_s^{v}(x,y)}. \tag{4.5}$$

The obtained amplitude and phase of $\widetilde{E}_s^{v}$ corresponding to the interference pattern in Fig. 4.9(a) are shown in Fig. 4.10. If the reference beam has uniform intensity $E_s^{v} = \widetilde{E}_s^{v}$ and we are done. In general, the reference beam intensity should be modelled as a Gaussian or separately measured, after which the correct signal field is obtained by dividing through the reference amplitude:

$$E_s^{v} = \widetilde{E}_s^{v}/|E_r^{v}|. \tag{4.6}$$

The procedure to obtain E_s^{h} from $\mathcal{F}\left\{E_s^{h}E_r^{h*}\right\}$ is analogous.

The signal-to-noise ratio (SNR) of our vector field detection is theoretically close to the shot noise limit. The shot noise limit can be reached by measuring the two polarization components on two separate cameras. Because we have both polarization components on a single camera the shot noise is increased by a factor $\sqrt{2}$, directly translating to a reduction in SNR of $\sqrt{2}$ [15]. Our choice of using a 50:50 beam splitter also reduces the SNR by $\sqrt{2}$. The fidelity of single-polarization off-axis holographic detection is at least $F \geq 0.99$, as is shown experimentally in e.g. Section 3.5. An SNR reduction by a factor 2 is negligible compared to e.g. the finite NA of our microscope objectives. Therefore, the great advantages such as compactness and ease of alignment of the two polarization components to each other make the choice for single-shot vector field detection on a single camera an easy one.

4.6 Mapping between vector field synthesis and detection

In the previous sections the various modules of the apparatus were discussed separately. In order to achieve accurate phase conjugation through a multiple-scattering medium the modules must be adequately aligned with respect to each other. In particular, the mapping between the vector field synthesis and detection modules is critical. We distinguish between two aspects of the alignment: calibration of the angles and mapping of the pixels between the vector field synthesis and detection modules.

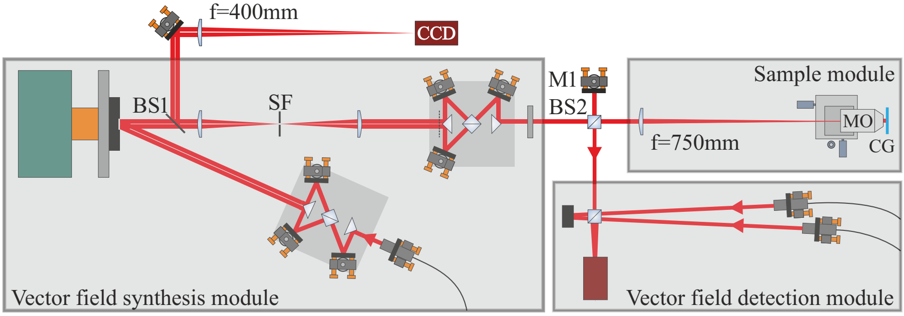


Figure 4.11: Schematic of one half of the apparatus. The synthesis, detection and sample modules are connected through a 50:50 cube beam splitter (BS2). Two additional mirrors, a lens, a CCD camera and 50:50 pellicle beam splitter (BS1) on a flip mount are used for angle calibration between the synthesis and detection modules.

4.6.1 Angle calibration

An angle mismatch as small as $0.01°$ between the normal vectors to the field synthesis and detection planes can cause a difference between the synthesized and detected fields of a full phase wrap over the extent of the modulator and detector chips. This can cause the phase conjugation fidelity F, defined as the inner product between the detected and synthesized fields, to drop to 0.

Our angle calibration procedure is explained with reference to Fig. 4.11, which schematically shows one half of the apparatus. We construct a plane wave using the vector field synthesis module. The module is assumed to be aligned such that the intermediate focus inside the spatial filter (SF) is positioned exactly at the center of the filter. The plane wave reflects from a 50:50 cube beam splitter (BS2). The transmitted beam is blocked during this alignment step. After reflection from mirror M1 half of the light is reflected back into the construction module. A 50:50 pellicle beam splitter and a lens with focal length $f = 400\,\mathrm{mm}$ are used to image the spatial filter to a CCD camera (Guppy F146-B). Mirror M1 is now aligned so that the reflected beam is focused exactly at the center of SF. This ensures that the reflected beam is the exact phase conjugate of the initial beam. The other half of the light that is reflected from mirror M1 is transmitted through BS2 and enters the detection module. We now know that the angle of this beam exactly matches the angle of the synthesis module. Therefore, we calibrate the off-axis holographic field detection such that this beam is mapped to the $k = 0$ plane wave. This procedure is performed separately for the vertical and horizontal field components.

4.6.2 Pixel mapping

Phase conjugation of a light field requires that we know for each pixel in the detection module to which pixel in the synthesis module it corresponds. The optics induces displacement, mirroring, scaling and rotation, which must be character-

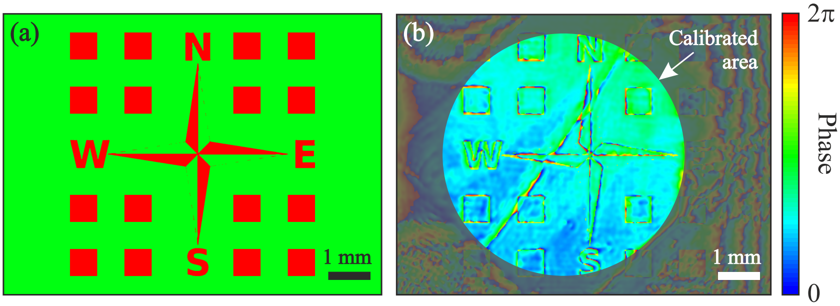


Figure 4.12: (a) Phase of the calibration field. (b) Difference between the phase of the desired field and the synthesized field as it is measured in the detection module. The calibration is optimal when the difference is constant up to a phase gradient caused by a tilt of the cover glass. We observe a well-calibrated area with a diameter of approximately 6 mm. The diagonal stripe is a scratch on the cover glass, used only for imaging the synthesis and detection modules onto the sample plane.

ized. In this calibration step, we block mirror M1 and unblock the beam that enters the sample module. We use a standard microscope cover glass (CG) as a reflecting surface in the sample plane. The synthesis and detection modules are both assumed to be sharply imaged to the cover glass.

A calibration field is defined that has a uniform intensity and the image of a compass with surrounding squares encoded in the phase. The phase pattern of the calibration field is shown in Fig. 4.12(a). We map this field to the detection module, where it exactly covers the chip of the CCD. The calibration now translates to solving the problem: suppose we measure this field on the detection module, then what do we need to write on the synthesis module to conjugate this field? The way to solve this is by writing the calibration field onto the synthesis module and then displacing, mirroring, scaling and rotating it until the field measured on the detection module is exactly equal to the desired calibration field. As a feedback we use an image that contains the phase difference between the desired calibration field and the measured synthesized field. Only when the calibration is correct we see that they cancel to have a phase profile that is uniform up to a phase gradient, as is shown in Fig. 4.12(b). The phase gradient is irrelevant here; it is caused by a slight tilt of the cover glass and does not influence the pixel mapping. The corresponding angles are calibrated differently, as described in Section 4.6.1. In the center we see a calibrated area with a diameter of approximately 6 mm size on the detection and synthesis modules. The alignment accuracy is in the order of a few CCD pixels. This is significantly better than a diffraction limited spot size and, therefore, good enough to perform accurate optical phase conjugation. An alignment fidelity $F > 0.8$ was obtained using a similar procedure in the pixel mapping performed for the experiment described in Section 5.2 and is not a fundamental limit of the apparatus. Additional adjustments to the pixel mapping can be made using the phase conjugated signal through a multiple-scattering medium as feedback. The pixel mapping procedure, like the angle calibration procedure, is performed separately for the vertical and horizontal field components.

4.7 Conclusion

In this chapter we described our apparatus for maximum control over the scattering matrix of a multiple-scattering medium in the spatial and frequency domain. The apparatus is designed to fulfill the requirements described in Section 4.1. A sample consisting of a 12 μm thick layer of ZnO nanoparticles satisfies all sample requirements. The light source can resolve modes with lifetimes of approximately 130 fs up to 0.2 ns, which is more than enough to resolve lifetimes that are shorter as well as much longer than the average lifetime of modes in our sample. The vector field synthesizers and detectors allow full control over the amplitude, phase and polarization of light in approximately 10^4 pixels, which is theoretically sufficient to cover the spatial extent of open channels and long-lived modes in the sample. The performance of the apparatus seems limited mainly by the optics. The NA of the oil immersion objective limits the phase conjugation fidelity to $F = 0.85$. Despite this limitation an overall phase conjugation fidelity of $F > 0.5$ seems entirely feasible. According to the predictions in Chapter 2, this is more than enough to achieve greatly enhanced coupling to open channels as well as long-lived modes. Therefore, we expect that the apparatus described in this chapter will enable landmark observations of important phenomena in multiple-scattering media.

Bibliography

[1] M. Burresi, F. Pratesi, F. Riboli, and D. S. Wiersma, *Complex photonic structures for light harvesting*, Adv. Opt. Mater. (online March 25, 2015). — p.45.

[2] A. P. Mosk, A. Lagendijk, G. Lerosey, and M. Fink, *Controlling waves in space and time for imaging and focusing in complex media*, Nature Photon. **6**, 283 (2012). — p.45.

[3] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, *The security of practical quantum key distribution*, Rev. Mod. Phys. **81**, 1301 (2009). — p.45.

[4] M. C. W. van Rossum and T. M. Nieuwenhuizen, *Multiple scattering of classical waves: microscopy, mesoscopy, and diffusion*, Rev. Mod. Phys. **71**, 313 (1999). — p.46.

[5] M. P. van Albada, B. A. van Tiggelen, A. Lagendijk, and A. Tip, *Speed of propagation of classical waves in strongly scattering media*, Phys. Rev. Lett. **66**, 3132 (1991). — p.46.

[6] New Focus user's manual, model TLB 6700-LN and TLB 6700-XP tunable diode laser, (2010), http://assets.newport.com/webDocuments-

EN/images/TLB-6700__User_Manual_Rev_D.pdf, accessed on March 2, 2015. — p.48.

[7] New Focus Velocity 6700 widely tunable lasers, datasheet, http://assets.newport.com/webDocuments-EN/images/DS_041104_Velocity_Datasheet.pdf, accessed on March 2, 2015. — p.48.

[8] New Focus tunable laser linewidth, technical note, http://assets.newport.com/webDocuments-EN/images/31626.pdf, accessed on March 2, 2015. — p.48.

[9] I. M. Vellekoop, *Controlling the propagation of light in disordered scattering media*, Ph.D. thesis, University of Twente, 2008. — p.51, 52.

[10] E. G. van Putten, *Disorder-enhanced imaging with spatially controlled light*, Ph.D. thesis, University of Twente, 2011. — p.52.

[11] A. B. Parthasarathy, K. K. Chu, T. N. Ford, and J. Mertz, *Quantitative phase imaging using a partitioned detection aperture*, Opt. Lett. **37**, 4062 (2012). — p.54.

[12] M. Takeda, H. Ina, and S. Kobayashi, *Fourier-transform method of fringe-pattern analysis for computer-based topography and interferometry*, J. Opt. Soc. Am. **72**, 156 (1982). — p.54.

[13] D. Akbulut, *Measurements of strong correlations in the transport of light through strongly scattering materials*, Ph.D. thesis, University of Twente, 2013. — p.54.

[14] T. Colomb, P. Dahlgren, D. Beghuin, E. Cuche, P. Marquet, and C. Depeursinge, *Polarization imaging by use of digital holography*, Appl. Opt. **41**, 27 (2002). — p.54.

[15] H. Yılmaz, W. L. Vos, and A. P. Mosk, *Optimal control of light propagation through multiple-scattering media in the presence of noise*, Biomed. Opt. Express **4**, 1759 (2013). — p.56.

CHAPTER 5

Quantum-secure authentication of a physical unclonable key

Authentication of persons and objects is a crucial aspect of security. We experimentally demonstrate Quantum-Secure Authentication (QSA) of a classical multiple-scattering key. The key is authenticated by illuminating it with a light pulse containing fewer photons than spatial degrees of freedom and verifying the spatial shape of the reflected light. Quantum-physical principles forbid an attacker to fully characterize the incident light pulse. Therefore, he cannot emulate the key by digitally constructing the expected optical response, even if all information about the key is publicly known. QSA offers a combination of highly desirable properties that is unmatched by any other authentication method. QSA uses a key that cannot be copied due to technological limitations and is quantum-secure against digital emulation. Moreover, QSA does not depend on secrecy of stored data, does not depend on unproven mathematical assumptions and is straightforward to implement with current technology.

5.1 Introduction

Authentication of persons can be based on "something that you know", e.g. digital keys, or "something that you have", e.g. physical objects such as classical keys or official documents. A drawback of digital keys is that their theft can go unnoticed; a drawback of traditional physical keys is that they can be copied secretly. A Physical Unclonable Function (PUF) is a physical object that cannot feasibly be copied because its manufacture inherently contains a large number of uncontrollable degrees of freedom. Making a sufficiently accurate clone or concocting a device that mimics its physical behavior is infeasible, though not theoretically impossible, given the properties of PUFs [1, 2]. See also Section 6.4. A PUF is a function in the sense that it reacts to a stimulus (challenge) by giving a response. After manufacture there is a one-time characterization of the PUF

This chapter has been published as: S.A. Goorden, M. Horstmann, A.P. Mosk, B. Škorić, and P.W.H. Pinkse, Optica **1**, 421–424 (2014)

in which its challenge-response behavior is stored in a database. The PUF (from this point referred to as the "key") can later be authenticated by comparing its response behavior to the database, see Fig. 5.1a.

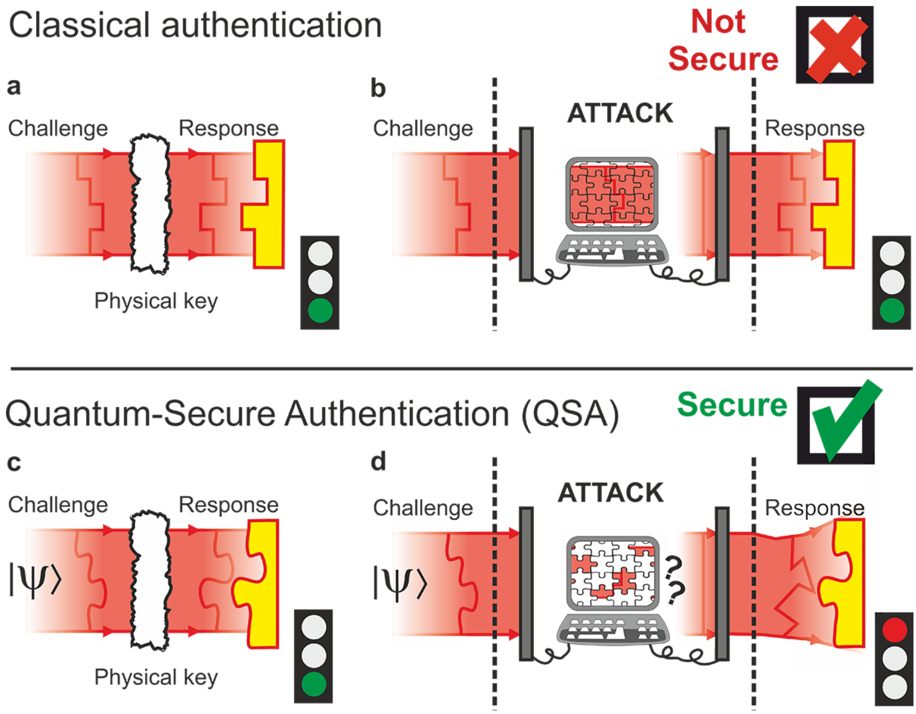


Figure 5.1: The idea of Quantum-Secure Authentication (QSA): (a) In classical authentication of an optical unclonable physical key, a challenge wavefront of sufficient complexity is sent to the key. The response wavefront is compared with those stored in a database (yellow pieces) to make a pass (green light) or fail (red light) decision. However, this verification can be spoofed by an emulation attack (b) in which the challenge wavefront is completely determined and the expected response is constructed by the adversary who knows the challenge-response behavior of the key. In Quantum-Secure Authentication (c) the challenge is a quantum state for which an emulation attack (d) fails because the adversary cannot actually determine the quantum state and hence any attempt to generate the correct response wavefront fails.

When they are read out classically, PUFs are vulnerable to a class of attacks that we will refer to as digital emulation (Fig. 5.1b). Here the adversary has knowledge of the key's properties either from physical inspection of the key or by access to the challenge-response database. He intercepts challenges and is able to provide the correct responses by looking them up in his database. This is a highly relevant scenario as accessible databases are notoriously difficult to protect. So far the only defense against digital emulation is to deploy various sensors that try to detect if some form of spoofing is going on. This leads to an expensive arms race in which it is difficult to ascertain the level of security.

In this chapter we present Quantum-Secure Authentication (QSA) of optical keys, a scheme with highly desirable properties: QSA

- uses a key that is infeasible to emulate physically,
- is unconditionally secure against digital emulation attacks,
- does not depend on secrecy of any stored data,
- does not depend on unproven mathematical assumptions,
- is straightforward to implement with current technology.

No comparable object authentication method currently exists. The use of quantum physics in QSA is inspired by quantum cryptography [3–5]. However, there are major differences. The aim of quantum cryptography is to generate a secret digital key known only to Alice and Bob, whereas QSA allows Alice to check if Bob possesses a unique physical object. Quantum cryptography requires the existence of an authenticated channel between Alice and Bob, typically based on a secret key that is shared beforehand [6]. In contrast, QSA needs only publicly available information; there are no secrets. See Section 6.2 for an overview of cryptographic primitives and their properties.

5.2 Implementation

Our implementation of QSA uses a three-dimensional random scattering medium as a PUF [1, 7, 8]. Details are provided in Appendix 5.A. The challenges are high-spatial-dimension states of light [9–11] with only a few photons. The response is speckle-like and depends strongly on the challenge and the positions of the scatterers. Due to the no-cloning theorem [12] it is impossible for an adversary to fully determine the challenge and therefore to construct the expected response (Fig. 5.1c-d). The verifier can, however, easily verify the presence of the encoded information with an appropriate basis transformation, authenticating the key.

After its manufacture, the key is enrolled: the challenge-response pairs are measured with as much light as needed. Each of our challenges is described by a 50×50 binary matrix. Each element corresponds to a phase of either 0 or π. A spatial light modulator (SLM1) is used to transform the incoming plane wavefront into the desired challenge wavefront. The challenge is sent to the key and the reflected field is recorded in a phase-sensitive way. The challenge along with the corresponding response is stored in a challenge-response database. In our current implementation this requires 20 kB of computer memory per challenge-response pair. Linearity of the system ensures that every superposition of challenge-response pairs is also a challenge-response pair. Storing a basis of challenge-response pairs, which requires 50 MB of computer memory in our implementation, is sufficient to fully characterize a key.

After enrolment, keys are authenticated using the setup illustrated in Fig. 5.2. The light source, spatial light modulators, pinhole and photon detector are part of the authentication device. In the current work, we assume the authentication

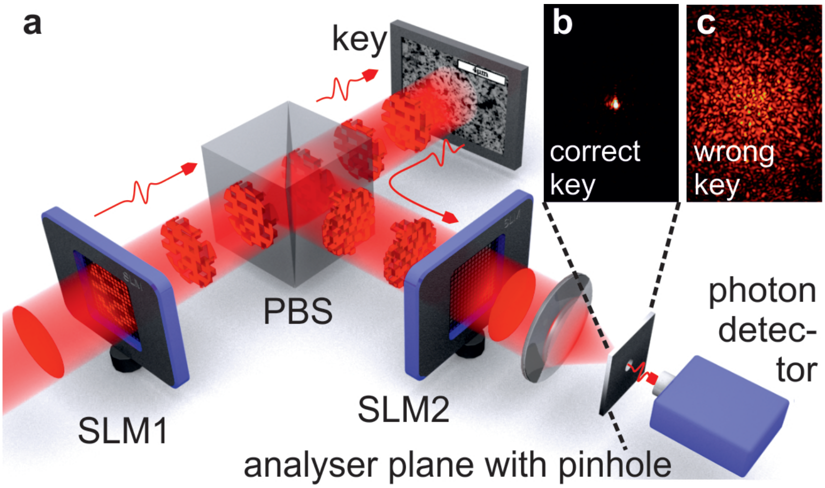


Figure 5.2: Quantum-secure optical readout of a physical key. (a) Setup: A spatial light modulator (SLM1) creates the challenge by phase shaping a few-photon wavefront. In the experiment a 50×50 binary phase pattern is used with 0 and π phase delays. The challenge is sent to the ZnO key (scale bar is 4 μm) by a microscope objective (not shown). The response is coupled out by a polarizing beam splitter (PBS). The response is transformed back by SLM2 and then focused onto the analyzer plane. (b) Only if the key is the true unique key, the response has a bright spot in the center, holding $\approx 60\%$ of the power in the image and allowing that fraction to pass a pinhole and land on a detector where photodetection clicks authenticate the key. (c) In case of a false key, the response in the analyzer plane is a random speckle pattern.

device is tamper-resistant. Our light source is an attenuated laser beam chopped into 500 ns light pulses each containing $n = 230 \pm 40$ photons. Quantum readout of optical keys can be achieved with single or bi-photon states [13], squeezed states [14] or other fragile quantum states [15]. We use coherent states of light with low mean photon number [16], because in QSA they provide a similar security as other quantum states and are easier to implement in real-life applications. A challenge-response pair is constructed using information from the database. SLM1 is used to shape the few-photon challenge wavefront, which is then sent to the key. The reflected wavefront is sent to SLM2, which adds to it the conjugate phase pattern of the expected response wavefront. Therefore, SLM2 transforms the reflected speckle field into a plane wave only when the response is correct. In case the response is wrong, SLM2 transforms the field into a completely different speckle field. When the response is correct, the lens positioned behind SLM2 focuses the plane wave to a point in the analyzer plane, as shown in Fig. 5.2b. A false key will result in a speckle on the analyzer plane as shown in Fig. 5.2c. Compared to the typical peak height in Fig. 5.2b of 1000 times the background, the loss of intensity in the center of Fig. 5.2c is dramatic. We spatially filter the field in the analyzer plane with a pinhole and image it onto a photon-counting detector.

5.3 Measurement results

In Fig. 5.3a we show the typical photodetector signal for the correct response and for an incorrect response provided by the true and a false key, respectively. Only with the true key multiple photodetections are seen. After repeating the measurement 2000 times, Fig. 5.3b shows the histogram of the number of photodetections for the true key, resembling a Poissonian distribution with a mean of 4.3. Fig. 5.3b also shows the average histogram of photodetections when 5000 random challenges are sent to the key, with the key and SLM2 kept unchanged. This experiment gives an upper bound on the photodetections in case of an attack with a random key. This histogram resembles a Poissonian distribution with a mean of 0.016 photodetections. We can clearly discriminate between true and false keys.

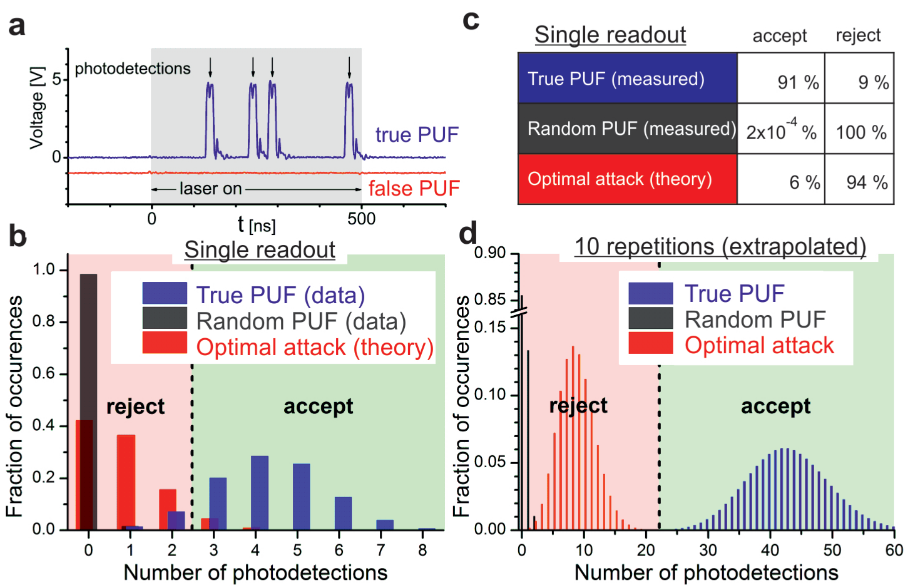


Figure 5.3: Quantum-secure readout of an unclonable physical key (PUF), using challenge pulses with 230 ± 40 photons distributed over 1100 ± 200 modes. (a) Real-time examples for the true key (blue line) and a false key (red line, offset for clarity). (b) Measured number of photodetections in case of the true key, a random key (imitated by sending random challenges to the same key), and for an optimal attack given $S = 4$. The threshold is chosen such that the false positive and negative probabilities are approximately equally small assuming an optimal attack. (c) Acceptance and rejection probabilities in case of the true key, a random key and in case of an optimal digital emulation attack. (d) Number of photodetections extrapolated to 10 repetitions: the false positive and false negative probabilities quickly decrease to order 0.01 %.

5.4 Security against challenge estimation attacks

In order to characterize the achievable security for one repetition of our readout, we introduce the quantum security parameter S,

$$S = K/n, \tag{5.1}$$

as the ratio of the number of controlled modes K and the average number of photons n in the challenge. The parameter K quantifies the dimensionality of the challenge space and is equal to the number of independent response wavefronts that are obtained by sending in different challenge wavefronts. It is well approximated by the number of speckles on the key illuminated by the challenge [17]. In our experiment we have $K = 1100 \pm 200$ and $n = 230 \pm 40$, yielding $S = 5 \pm 1$. Because a measurement of a photon can extract only a limited amount of information, a large S implies that the adversary can only obtain a small fraction of the information required to characterize the challenge. Therefore he cannot determine the correct response. For quantum state estimation attacks based on various classes of measurements it has been shown [18–20] that the adversary cannot achieve a fidelity better than approximately

$$F = F_{\mathrm{OK}}/(S + 1), \tag{5.2}$$

where F is the fraction of photons detected by the verifiers hardware in case of an attack and F_{OK} is the fraction of photons detected when the response is correct. (The attack classes covered in the existing proofs are very broad and include e.g. field quadrature measurements, which are believed to optimally extract information from coherent states.)

The result (5.2) holds for $S > 1$ and $K \gg 1$ and is in line with the intuition that a measurement of n photons can only provide information about n modes. Operating the readout in the regime $S > 1$ therefore gives the verifier an eminent security advantage which has its origin in the quantum character of light. In the verification we aim to discriminate a correct key from an optimal attack. Given a conservative lower bound of $S = 4$, the number of photodetections on the single-photon detector in a single readout in case of an optimal (digital emulation) attack follows a Poissonian distribution with mean 0.86, as shown in Fig. 5.3b. We assume that the attacker returns within the statistical error the correct total number of photons, which can be ensured by counting the photons that miss the pinhole. Choosing a threshold of 3 or more photodetections for accepting the key, we find that the measured false reject ratio is 9%. In case of random challenges the false accept ratio is $1.7 \times 10^{-4}\%$ and the theoretical maximum false accept probability in case of the digital emulation attack (Eq. 5.2) is 6% (Fig. 5.3c). The security improves exponentially by repeating the verification, every time choosing a different challenge and its corresponding SLM2 setting from the database. The individual photon counts are added, and a combined threshold is set. As illustrated in Fig. 5.3d, after 10 repetitions the false accept and false reject probabilities are of order 10^{-4}. As detailed in Appendix 5.B, after 20 repetitions they are both of order 10^{-9}. Thus, the false decision rates can be made negligible in a small number of repetitions.

5.5 Conclusion

In our implementation, the time for readout is limited to about 100 ms by the switching time of the SLM. Using faster micromirror-based SLMs [21, 22], the complete authentication protocol with 20 repetitions can be performed in less than a millisecond. The one-time enrolment of the key then takes on the order of a second. Quantum-secure authentication does not require any secret information and is therefore invulnerable to adversaries characterizing the properties of the key (skimming). Hence, QSA provides a practical way of realizing unprecedentedly secure authentication of IDs, credit cards, biometrics [23] and communication partners in quantum cryptography.

5.A The key

Our PUF consists of zinc-oxide (ZnO) nanoparticles with an average grain size of 200 nm and air. The samples are created by spray painting, using a method described in detail in [24]. The transport mean free path of such samples is $l_{\mathrm{tr}} = 0.7 \pm 0.2\mu$m. We use the key in reflection geometry because it is practical in real-life applications and collect the cross-polarized light to ensure multiple scattering in the bulk of the key. We illuminate a circular area with a diameter of approximately 15 μm on the surface of the key and collect light from an area with a diameter of approximately 25 μm.

5.B Repetition for exponential security gain

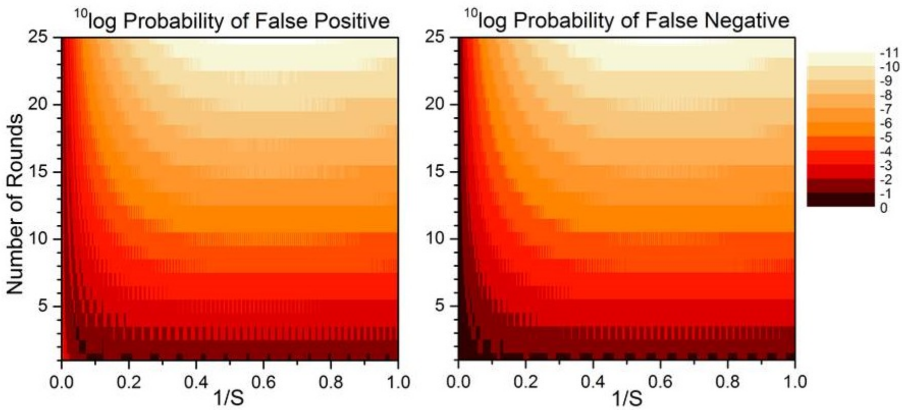


Figure 5.4: Probability of a false positive (acceptance of a challenge estimation attack) and a false negative decision (rejection of a correct PUF) as a function of the security parameter S and the number of repetitions (rounds). The plot is made by varying n and choosing the optimal threshold, while keeping $K = 1062$.

Fig. 5.4 shows the calculated probability of false-positive and false-negative decisions as a function of S and the number of repetitions, with the number of modes K kept constant. For each point in Fig. 5.4 the threshold was chosen in the minimum between the photon detection distributions obtained with the true PUF and the one calculated for the optimal challenge estimation attack. This leads to false positive and false negative probabilities that are approximately equally small. At a moderate S the probability of an erroneous decision is already of order 10^{-4} after 10 repetitions. At high S it takes more repetitions to rule out incorrect decisions since high S (at fixed K) implies a low photon number n. Since the threshold can only be taken at an integer number of photons, one may notice some quantization steps. For larger numbers of repetitions the probability of an incorrect decision is reduced exponentially and can hence be made arbitrarily small.

Bibliography

[1] R. Pappu, B. Recht, J. Taylor, and N. Gershenfeld, *Physical one-way functions*, Science **297**, 2026 (2002). — p.61, 63.

[2] J. D. R. Buchanan, R. P. Cowburn, A. Jausovec, D. Petit, P. Seem, G. Xiong, D. Atkinson, K. Fenton, D. A. Allwood, and M. T. Bryan, *Forgery: 'fingerprinting' documents and packaging*, Nature **436**, 475 (2005). — p.61.

[3] C. H. Bennett, G. Brassard, S. Breidbard, and S. Wiesner, *Quantum cryptography, or unforgeable subway tokens*, Advances in Cryptology: Proc. CRYPTO '82 267 (1982). — p.63.

[4] C. H. Bennett and G. Brassard, *Quantum cryptography: Public key distribution and coin tossing*, IEEE International Conference on Computers, Systems and Signal Processing 175 (1984). — p.63.

[5] B. Škorić, *Quantum readout of physical unclonable functions*, Int. J. Quant. Inf. **10**, 1250001 (2012). — p.63.

[6] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, *The security of practical quantum key distribution*, Rev. Mod. Phys. **81**, 1301 (2009). — p.63.

[7] B. Škorić, P. Tuyls, and W. Ophey, *Robust key extraction from physical uncloneable functions*, in Applied Cryptography and Network Security (ACNS), Vol. 3531 of LNCS (Springer, New York, U.S.A., 2005) 407 . — p.63.

[8] P. Tuyls, B. Škorić, S. Stallinga, A. H. M. Akkermans, and W. Ophey, *Information-theoretic security analysis of physical uncloneable functions*, in Financial Cryptography and Data Security, Vol. 3570 of LNCS (Springer-Verlag Berlin Heidelberg, Germany, 2005) 141 . — p.63.

[9] S. P. Walborn, D. S. Lemelle, M. P. Almeida, and P. H. Souto Ribeiro, *Quantum key distribution with higher-order alphabets using spatially encoded qudits*, Phys. Rev. Lett. **96**, 090501 (2006). — p.63.

[10] V. D. Salakhutdinov, E. R. Eliel, and W. Löffler, *Full-field quantum corre-*

lations of spatially entangled photons, Phys. Rev. Lett. **108**, 173604 (2012). — p.63.

[11] S. Etcheverry, G. Cañas, E. S. Gómez, W. A. T. Nogueira, C. Saavedra, G. B. Xavier, and G. Lima, *Quantum key distribution session with 16-dimensional photonic states*, Sci. Rep. **3**, 2316 (2013). — p.63.

[12] W. K. Wootters and W. H. Zurek, *A single quantum cannot be cloned*, Nature **299**, 802 (1982). — p.63.

[13] A. Peruzzo, M. Lobino, J. C. F. Matthews, N. Matsuda, A. Politi, K. Poulios, X.-Q. Zhou, Y. Lahini, N. Ismail, K. Wörhoff, Y. Bromberg, Y. Silberberg, M. G. Thompson, and J. L. O'Brien, *Quantum walks of correlated photons*, Science **329**, 1500 (2010). — p.64.

[14] L.-A. Wu, H. J. Kimble, J. L. Hall, and H. Wu, *Generation of squeezed states by parametric down conversion*, Phys. Rev. Lett. **57**, 2520 (1986). — p.64.

[15] D. Bouwmeester, A. Ekert, and A. Zeilinger, *The physics of quantum information* (Springer-Verlag Berlin Heidelberg, Germany, 2000). — p.64.

[16] P. W. H. Pinkse, T. Fischer, P. Maunz, and G. Rempe, *Trapping an atom with single photons*, Nature **404**, 365 (2000). — p.64.

[17] J. F. de Boer, M. C. W. van Rossum, M. P. van Albada, T. M. Nieuwenhuizen, and A. Lagendijk, *Probability distribution of multiple scattered light measured in total transmission*, Phys. Rev. Lett. **73**, 2567 (1994). — p.66.

[18] B. Škorić, A. P. Mosk, and P. W. H. Pinkse, *Security of quantum-readout PUFs against quadrature-based challenge-estimation attacks*, Int. J. Quant. Inf. **11**, 1350041 (2013). — p.66.

[19] D. Bruß and C. Macchiavello, *Optimal state estimation for d-dimensional quantum systems*, Phys. Lett. A **253**, 249 (1999). — p.66.

[20] B. Škorić, *Security analysis of quantum-readout PUFs in the case of challenge-estimation attacks*, submitted, http://eprint.iacr.org/2013/479 (2013). — p.66.

[21] D. Akbulut, T. J. Huisman, E. G. van Putten, W. L. Vos, and A. P. Mosk, *Focusing light through random photonic media by binary amplitude modulation*, Opt. Express **19**, 4017 (2011). — p.67.

[22] D. B. Conkey, A. M. Caravaca-Aguirre, and R. Piestun, *High-speed scattering medium characterization with application to focusing light through turbid media*, Opt. Express **20**, 1733 (2012). — p.67.

[23] I. M. Vellekoop and A. P. Mosk, *Focusing coherent light through opaque strongly scattering media*, Opt. Lett. **32**, 2309 (2007). — p.67.

[24] E. G. van Putten, *Disorder-enhanced imaging with spatially controlled light*, Ph.D. thesis, University of Twente, 2011. — p.67.

CHAPTER 6

Implementation and valorization of quantum-secure authentication

6.1 Introduction

International news in recent years is increasingly dominated by threats to security related to our arrival in the digital age [1, 2]. A few examples that are reported frequently are counterfeiting, data leaks, money theft, unauthorized access and identity theft. The common denominator of all these problems is that they arise due to failure in authentication of persons or objects.

Quantum physics can be used to enhance security. Notably, Quantum Key Distribution (QKD) methods, sometimes referred to as quantum cryptography, are succesful in solving the problem of secure message encryption [3]. QKD research is blooming and QKD systems are now commercially available. A natural question is whether quantum physics can be harnessed to achieve a similar effect in the field of object authentication.

Quantum-Secure Authentication (QSA) of a physical unclonable key, described in Chapter 5, exploits the quantum nature of light to obtain the most secure practical object authentication method available today. It is a rare opportunity that we can use a fundamental law of physics, in this case quantum physics, to solve a problem with such direct importance in society. In this chapter, we will further explore the potential impact of QSA.

In Section 6.2 we give an overview of a number of important security primitives. In Section 6.3 we discuss recent security breaches caused by insecure authentication. An in-depth analysis of potential security risks and countermeasures in QSA is provided in Section 6.4. Finally, in Section 6.5 we describe how we plan to bring QSA to the market.

6.2 Authentication and other cryptographic methods

Authentication is important throughout society. You are authenticated every day when unlocking your house or car, logging into your phone, mailbox, Facebook or any other website and when using a card to buy something in a shop or online. In order to understand how this is done and to help us place QSA into its security

Parts of this chapter are adapted from the supplementary information of S.A. Goorden, M. Horstmann, A.P. Mosk, B. Škorić, and P.W.H. Pinkse, Optica **1**, 421–424 (2014) context, we provide an overview of cryptographic methods and their purpose, strengths and weaknesses.

6.2.1 Object authentication methods

Methods for authenticating persons and objects can typically be placed in one of three categories: methods based on "something you know", "something you are" or "something you have".

Something you know

- **Passwords and pass phrases** are very widely used for authentication of persons. They require that the password / pass phrase is kept secret and difficult to guess.

- **PIN codes** are very widely used for authentication of persons. They require that the PIN code is kept secret and difficult to guess.

Something you are

- **Signatures** are very widely used for authentication of persons. They require that a signature is difficult to copy and that information about the signature is not widespread.

- **Fingerprint** verification is a common biometric authentication method. It requires measurement and secret storage of fingerprint information. In case an attacker knows information about the fingerprint, the fingerprint is relatively straightforward to copy. Privacy is a great concern with fingerprints and other biometric authentication methods.

- **Iris scanning** is a biometric authentication method, very similar to fingerprint verification. Because the iris is better protected than a fingerprint, the iris scan is more accurate. Although it is more difficult than for the fingerprint, an attacker can use an image of the iris to spoof the iris scanner if he has the information of the iris.

Something you have

- **Mechanical keys** are very widely used for access control to e.g. houses and cars. It requires a physical lock and key mechanism as well as distribution of physical keys. The security is based on the assumption that inferring the key from the lock is difficult. In case an attacker knows information about the key, the key is relatively straightforward to copy.

- **Chip cards and RFID chips** are widely used in e.g. bank cards, passports and access cards. The chip contains a secret key that can be verified. A requirement is that the key remains secret. Classical cryptographic methods, such as described in Section 6.2.2, are often used to verify the key without directly transmitting the key. In case an attacker knows the key, it is relatively straightforward to copy the chip.

- **Classical authentication of a Physical Unclonable Function (PUF)** [4, 5] is a class of modern object authentication methods based on PUFs. A PUF is a physical object that exhibits a “challenge-response behavior”: if it is presented with a challenge (essentially a question) it will provide a response (the corresponding answer). The defining properties of PUFs are identifiability and physical unclonability. Identifiability means that PUFs can be recognized by verifying their challenge-response behavior, which is typically the case when the challenge-response behavior is reproducible and when all PUFs are unique. Physical unclonability means that it is assumed to be impossible to make an exact copy of a PUF due to technological limitations. This property is typically induced by uncontrollable randomness in the process of creating a PUF. There are many objects that exhibit these properties and are therefore considered PUFs [4]. Although they are by definition physically unclonable, PUFs are in general not mathematically unclonable. This means it is possible to create a mathematical description of the challenge-response behavior of the PUF. This allows an attacker to copy its behavior by alternative means, i.e. to digitally emulate the PUF. According to Ref. [4] the only type of PUF that is both physically as well as mathematically unclonable is the optical PUF. The underlying assumption is that large optical PUFs are too complex to fully characterize. However, like for other PUFs, production of an optical PUF is followed by an enrollment phase in which its challenge-response behavior must be characterized on a part of the challenge space. If an attacker knows which part of the challenge-response behavior of the PUF is characterized in the enrollment phase, for example by hacking the entity that produced and enrolled the PUF or an entity that wishes to authenticate the PUF, this allows him to digitally emulate the PUF. Therefore, classical authentication of a PUF is only possible if information about its challenge-response behavior remains secret or if anti-spoofing sensors are implemented to verify that the PUF is a PUF and not an emulation device. The latter leads to a tedious and expensive arms race in which security cannot be ascertained. Various PUF implementations have been experimentally demonstrated, but they have not yet been widely adopted.

- **Quantum money** [6, 7] exploits quantum memory for object authentication. Authentication of quantum money does not rely on mathematical or physical assumptions, but does require long-term storage and high fidelity initialization and readout of quantum memory. This is very difficult and expensive with current technology [8]. Quantum money is not yet demonstrated even as a laboratory experiment.

- **QSA** is a recently demonstrated object authentication method, described in Chapter 5. The optical readout process is required to use fewer photons than optical modes. QSA is secure under the assumption that lossless implementation of high-dimensional arbitrary optical unitary transformations is infeasible.

6.2.2 Message authentication methods

The methods described in this section are typically used for message authentication and encryption. They are, however, important for object authentication, because they can secure the communication between e.g. a verifier and a chip card.

- **Message Authentication Codes (MACs)** [9] are codes added to a digital message to identify the sender and to verify that the message has not been tampered with. MACs are unconditionally secure and widely used. The drawback is the requirement that a pre-shared key be distributed and secretly stored between *every pair* of parties that wishes to communicate.

- **RSA** [10] is a widely used public-key data encryption protocol, or cipher. It provides authentication of the sender by means of a digital signature. The great advantage of RSA is that it does not require distribution of secret keys. However, RSA relies on the mathematical assumption that factoring a product of two large primes is difficult on a classical computer and the physical assumption that quantum-computers are infeasible to build. RSA requires keeping the private key secret. Our current internet security relies on RSA.

- **McEliece** [11] is another cipher. It is an alternative to RSA, providing public-key encryption and digital signatures. It is based on the mathematical assumption that decoding an unknown linear code is difficult. It is a post-quantum crypto method, for which no attacks on a quantum-computer are known. McEliece is, however, considered less practical than RSA due to its larger key size.

- **Diffie-Hellman** [12] is a method for creating a shared secret key between two parties. This key can be used for symmetric message encryption. Diffie-Hellman relies on the mathematical assumption that discrete logarithms are difficult to compute and on the physical assumption that quantum-computers are infeasible to build. In order to authenticate the other party Diffie-Hellman requires an authenticated classical communication channel, using e.g. a short initial shared secret key or a certificate.

6.2.3 Quantum Key Distribution

Quantum key distribution (QKD) methods are used by authenticated parties to send encrypted messages to each other. Although QKD methods cannot be used to authenticate objects, they are mentioned here for their great importance in secure communication and close relation to QSA. We mention two of the most prominent methods in this booming field:

- **BB84** [3] is the oldest quantum key distribution method. Its purpose is to create a shared secret key between two parties, which can later be used to send an encrypted message. BB84 is unconditionally secure, which means it does not rely on any mathematical or physical assumptions. This method is commercially available. BB84 requires an authenticated classical communication channel, often based on a short shared secret key, to authenticate the other party.
- **SARG04** [13] is a modern quantum key distribution method, very similar to BB84. It implements weak coherent pulses instead of single photons, allowing key distribution over longer distances. SARG04 requires an authenticated classical communication channel.

6.2.4 Comparison of methods

We compare the above methods from the perspective of object authentication. Quantum key distribution methods such as BB84 and SARG04 do not perform object authentication. Quantum money is a promising object authentication method, but has not been demonstrated even in a laboratory environment and requires major technological improvements before it can become practical. Other methods mentioned in this section can also be used for object authentication, but rely on keeping information about the key secret. Passwords and PIN codes are immediately broken when the key leaks. Although it is a bit more difficult, traditional mechanical keys, signatures and biometric keys can also be copied when the information about the key is known. The same holds for chip cards and RFID chips, irrespective of classical cryptographic methods used to enhance their security. A classically authenticated PUF cannot be copied due to technological limitations, but digital emulation forms a major risk when its challenge-response behavior is known.

QSA uses a key that cannot be copied or digitally emulated, even if all information about the key is allowed to be publicly known. Considering the difficulty of keeping keys secret, as shown throughout Section 6.3, this is of major importance. Additional advantages are that the method does not rely on unproven mathematical assumptions and is relatively straightforward to implement. This highly desirable combination of properties sets QSA apart from other methods and makes it a valuable authentication primitive.

6.2.5 Multi-factor authentication

In multi-factor authentication, two or more elements from the “something you know”, “something you are” and “something you have” classes are combined to enhance security. Among multi-factor authentication methods, two-factor authentication is currently dominant. For example, it is widely used when withdrawing money using a bank card in combination with a PIN code. Combining two, three or even up to five factors yields increasing levels of security.

The explosive growth of the multi-factor authentication market, due to its wide support and wide variety of applications, offers great opportunities. An annual growth rate of 20% is expected during 2015-2020, resulting in a market of $10.75 billion by 2020 [14, 15].

The strength of a multi-factor authentication procedure depends on the strength of its factors. Three-factor authentication comprised of factors that are easy to exploit is not as strong as two-factor authentication with two strong factors. An ideal authentication procedure would require only a single unbreakable factor. Therefore, stronger authentication primitives are highly welcomed.

6.3 Security threats

In this section we highlight a number of authentication-related security threats that gather a large amount of media attention. This helps us understand what frequently goes wrong in authentication and how QSA can help address these problems.

6.3.1 Bank card fraud

A large number of people are affected by bank card fraud. The amount of money stolen through bank card fraud is increasing rapidly. In 2012 the worldwide loss amounted to over $11 billion, see Fig. 6.1. In a 2012 research it turned out that on average 27% of people experienced bank card fraud, with excesses of over 40% in the United States and Mexico [16].

Figure 6.1: The amount of money lost due to bank card fraud, image reprinted with permission from [17].

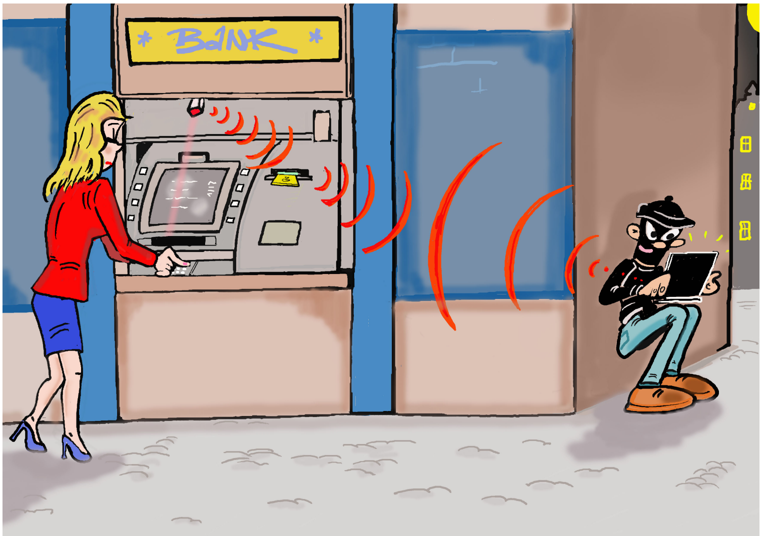


Figure 6.2: Illustration of skimming of a bank card. A pinhole camera views the PIN code and a skimming device retrieves the magnetic stripe data. The data are transported wirelessly.

Theft of authentication information is the key to bank card fraud. This is accomplished in a variety of ways. A common method is “skimming” of a bank card for which a great diversity of skimming devices has been employed [18]. Attackers use skimming devices to read the magnetic stripe information of a bank card, in combination with small pinhole cameras or fake keypads to retrieve the PIN code corresponding to the bank card. The information is, for example, wirelessly transmitted to the attacker. This process is illustrated in Fig. 6.2. A newer development is attackers installing malicious software, which captures the magnetic stripe information from the memory, on paying terminals. Rather than physically altering individual devices, they install this software on hundreds of devices at the same time. To illustrate the scale of this problem, attackers used such a method to obtain the authentication information of about 40 million bank cards in an attack on the United States retail giant Target in December 2013 [19]. The bank card information is then sold on online criminal marketplaces, alongside other sensitive authentication information [2, 20]. After obtaining the information it is relatively straightforward to make physical copies of the cards and empty the victims’ bank accounts.

Large scale attacks by malevolent organizations of hundreds of people take place against prepaid bank cards. The attackers obtained access to the computer systems of RBS WorldPay, in 2008, and of Fidelity National Information Services Inc., in 2011, allowing them to increase or remove the withdrawal limits of the bank cards. They distributed copies of these bank cards among hundreds of people in a large number of cities, who all simultaneously started withdrawing money from the same cards. In this way, they got hold of $9 million in the 2008 case and $13 million in the 2011 case [19, 21].

EMV chip cards, originally conceived by the companies Europay, Mastercard and Visa, have replaced magnetic stripe cards in Europe and are currently being adopted in the rest of the world. These cards use a microprocessor, which contains a secret number, for authentication of the card. The basic working principle for authentication of such a card is that the terminal sends a random number to the card, which the card combines with its own secret number. The card sends the response back, after which the bank checks whether the response is correct [22]. The idea behind this procedure is that eavesdropping on valid transactions does not help the attacker to make illegal transactions, because the random input from the terminal is always changing. Current attacks against EMV cards exploit weaknesses in the implementation of EMV card authentication. An example of such a weakness is the usage of poor random number generators, which make it much easier for an attacker to provide the correct response to the bank [22].

Attackers tend to exploit those weaknesses that require the smallest amount of effort. With the advent of EMV-enabled ATMs in Europe, two trends are observed. The first is that attackers move to parts of the world where they can find terminals that are not yet EMV-compatible and therefore allow magnetic stripe transactions. They can empty European bank accounts by withdrawing money in, e.g., the USA. Attackers also exploit flaws in the implementation of the relatively new and complex EMV system. These easily exploitable loopholes will be patched with time, after which attackers are likely to turn their attention towards creating direct copies of EMV cards. The secret cryptographic keys stored on EMV chips can be obtained in a variety of ways, including hacking of the computer system of the producer of the chip [23, 24] or reverse engineering of the chip [25, 26]. Any current model EMV card can be copied after obtaining the cryptographic key stored on the card.

6.3.2 Heartbleed

Leakage of authentication information is a great security risk. Leaked information can include passwords, private keys for digital signatures and EMV chip codes that allow copying the chip without ever even having access to it. Besides money theft, such information allows attackers to steal your identity, impersonate government or bank websites, and many other things. We highlight one event that dominated the news worldwide in 2014: Heartbleed.

Heartbleed is a software bug that leaks information from websites, e-mail servers and other online services [1, 28]. Ironically, the bug is part of OpenSSL, which is responsible for secure online communication. The bug is present in software versions from March 2012 until it was found by Google's Neel Mehta in March 2014 and publicly disclosed in April 2014 [29]. The Heartbleed bug in OpenSSL's Heartbeat extension is reported to be present in half a million [30] or 25-50% [28] of widely trusted websites.

When a client is communicating with such a website, typically indicated by "https://" in a browser's address bar, OpenSSL's Heartbeat extension checks continuity of the communication. The bug is related to a line of code in which

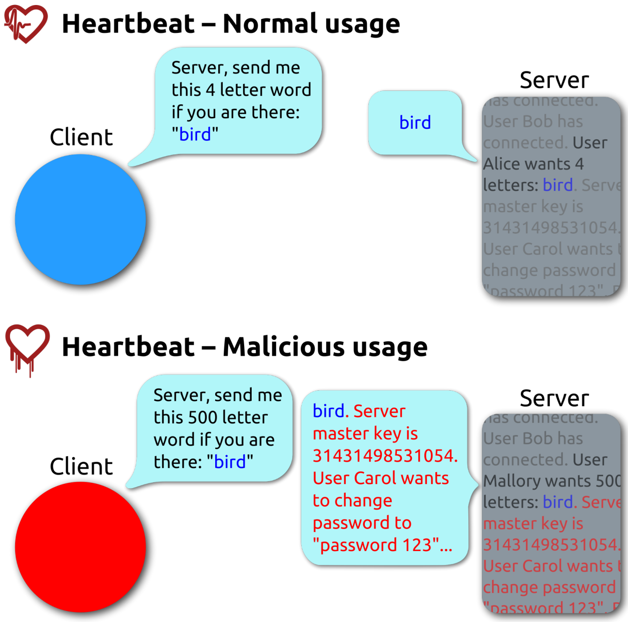


Figure 6.3: Simplified heartbleed explanation [27].

the client asks the server of the website to return a particular string and, at the same time, specifies the length of this string. The problem is that the server does not check whether the actual length and the specified length of the string match. In case the specified length is greater than the actual length of the string, the server leaks an amount of information from its memory which corresponds to the difference in lengths. This process is illustrated in Fig. 6.3.

The impact of Heartbleed was huge for a number of reasons. First, the leaked information contains highly sensitive authentication information including user passwords and private cryptographic keys. This allows attackers to act as the user or, even worse, to act as the supposedly secure website. Moreover, the bug was very widespread and easy to exploit on a large scale. Finally, exploiting it in principle does not leave traces, making it very difficult to determine to which extent it was exploited.

As a response to the disclosure of the bug, users worldwide were strongly advised to change their passwords and vulnerable servers had to upgrade OpenSSL and renew their potentially compromised authentication certificates. The total financial cost of this operation is very difficult to measure, but estimates are in the order of $500 million [31, 32]. The biggest known data breach believed to be caused by Heartbleed leaked 4.5 million patient records from the United States Community Health Systems [33]. In case criminals had been aware of and exploited the Heartbleed bug before its public disclosure, of which there is currently no evidence, the effects could have been truly disastrous. The example of Heartbleed shows that widespread software vulnerabilities are another reason why one cannot rely on secret information for secure authentication.

6.3.3 NSA and other government organizations

Some of the ways in which well-resourced organizations can break current authentication methods become clear by investigating strategies employed by government organizations. The United States National Security Agency (NSA), which has an estimated 40.000 employees and an annual budget of around $11 billion [34], is an example of an organization with a large amount of resources. The NSA's mission is "to protect U.S. national security systems and to produce foreign signals intelligence information" [35]. Besides its defensive mission of helping to protect the United States, the NSA has the crucial task of collecting information regarding the rest of the world and to provide infrastructure for targeted attacks. An important aspect of this task is to be able to break or circumvent authentication and encryption.

Software weaknesses are sought after and exploited by the NSA to advance their mission. In the attack against Iran's nuclear program using the Stuxnet virus in 2010, four such weaknesses were used [1]. The NSA is reported to have known about and exploited the Heartbleed bug to obtain authentication and other information for two years [36]. Besides exploiting software weaknesses, the NSA is accused of actively introducing such weaknesses for their own use [37, 38].

Authentication information including encryption keys and our passwords stored by U.S. based companies is directly accessed by the NSA, either by coercing these companies or without them being aware. Lavabit, a company providing encrypted email services to 410.000 people, shut down in summer 2013 after being ordered to hand over encryption keys [39, 40]. From classified documents leaked by former NSA contractor Edward Snowden in June 2013, we know that the NSA has direct access to authentication and other information on the servers of companies including Microsoft, Google, Apple and Facebook, covering an overwhelming fraction of email, video, search and other popular online services [41–43].

Also authentication information at companies outside the United States is not secure. Leaked documents show that the NSA and the British intelligence agency GCHQ breached the computer network of the Dutch chip-maker Gemalto [23, 24]. Gemalto is the worldwide leader in the production of SIM cards, used for authentication of mobile telephones and encryption of communication. They also produce smartcards including the EMV chips in modern bank cards. The intelligence agencies obtained the secret cryptographic keys that correspond to large badges of SIM cards directly from Gemalto, providing them unlimited access to the communication performed with the corresponding telephones.

Man-in-the-middle and man-on-the-side strategies, which are possible when the authentication process between communicating parties is not secure, are taking a prominent role in the NSA's arsenal. For example, when someone is logging in to Facebook, the NSA can send a response to this person before Facebook does. The person thinks he is communicating to a Facebook server, while in reality it is an NSA server. The NSA can exploit this situation to do a variety of things, such as installing malware on the victim's computer. According to a leaked NSA document these strategies have success rates as high as 80% [44, 45].

Malware was previously used by the NSA on a small and selective scale, where implants were operated individually by human NSA agents. Leaked NSA documents prove that they developed an infrastructure called TURBINE, which performs automated implantation of malware on groups of computers. This allows the network of computers with implants to rapidly grow to millions of implants, with no apparent limit other than the number of computers in the world. The implants come with a variety of "plug-ins", for example allowing the NSA to use the victim's microphone and webcam, read harddrives and flash drives and record key strokes [44]. Among other things, this allows them to obtain more authentication information.

Spoofing authentication methods provides the NSA immense power over the world's computer infrastructure. By pretending to be anyone they want they can achieve virtually anything they want. The NSA is currently the strongest player in this field, but the same methods are available to companies and criminals and are increasingly used by other governments [46]. Moreover, software bugs and malware and spyware vulnerabilities introduced by one party can also, perhaps even more easily, be exploited by other parties. Even if one decides to trust the NSA a major security risk is apparent, as our authentication and other private information may not be secure from anyone.

6.3.4 Would QSA help?

The authentication threats and breaches described in this section have in common that they are enabled by leaked authentication information. Since QSA does not depend on secrecy of the key information, it is immune to attacks described in this section. QSA can be directly implemented to secure e.g. bank cards and access cards. Although use of QSA for remote or online authentication has not yet been demonstrated, this is in principle possible by employing e.g. multimode fibers or fiber bundles to transmit challenges and responses between the verifier and the key.

6.4 Security analysis of QSA

Before and during implementation of a new security primitive in society, it is crucial to carefully investigate potential security breaches. An adversary who does not have the PUF may attempt several attack strategies. We address them here and show why they fail.

6.4.1 Blinding attacks

In a blinding attack, an adversary floods the system with light. This simple type of attack can be very powerful, exemplified by the fact that a QKD implementation has successfully been attacked by blinding the detectors [47]. An additional detector which measures the total intensity outside the pinhole is sufficient to prevent false positive detections. In addition, flooding can be detected by including fake challenges, for which no photon detections are expected. The time needed for one repetition of the procedure is in practice limited only by the switching time of the SLM, which is on the order of 100 ms for the current SLM but is orders of magnitude faster for e.g. digital micromirror devices. Therefore, there is ample room to randomly include fake challenges where (unknown to the adversary) no signal is expected. This also provides security against attacks that trigger the photodetector by non-optical means such as a beam of ionizing radiation.

6.4.2 Digital emulation attacks

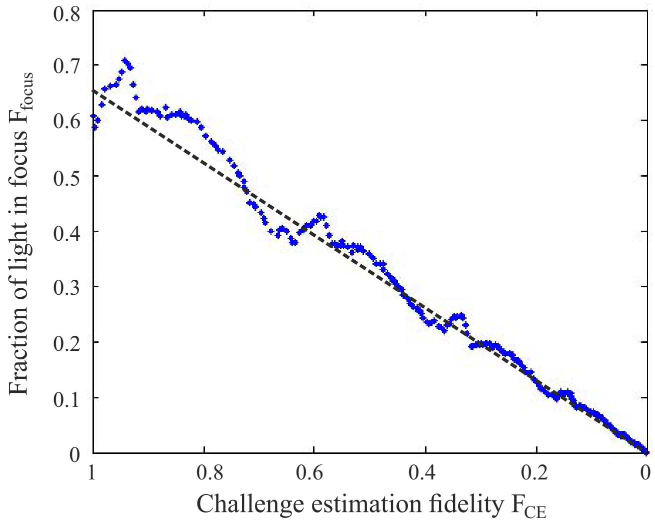


Figure 6.4: Experimental result showing the fraction of light focused onto the detector of the QSA device as function of the challenge-estimation fidelity reached by a simulated challenge-estimation attack.

A digital emulation attack is an attack in which the adversary attempts to measure the challenge and then looks up the response. As shown in [48] for single photon states and in [49] for quadrature measurements, this has a strictly limited probability of success, so that repeated authentications are exponentially likely to fail. A newer result [50] shows that when a challenge consists of $n < K$ quanta in the same state, our method is secure against all challenge-estimation attacks. A quantitative example shows what the adversary can hope to achieve: In the experiment shown in Chapter 5 the lower bound for the quantum security parameter $S = \frac{K}{n}$ is 4. Assuming that the adversary has a perfect photon-counting or quadrature measuring camera, the expected fidelity of the adversary's best estimate of the challenge is equal to $1/(S+1) = 1/5$ [49]. He can therefore expect to obtain a number of photon clicks at the detector that is 1/5 times the expected number of clicks with the correct challenge.

We experimentally tested the scaling at the basis of this argument. We parameterize the challenge wavefronts by a K-dimensional complex vector C_0. This C_0 is chosen by the verifier to yield the maximum light power in the focus behind SLM2 given the presence of the true PUF and the setting of SLM2. Now assume C_0 is replaced by the adversary's best challenge estimation C_1. We quantify the proximity of the estimated challenge C_1 to the original challenge C_0 by the challenge estimation fidelity $F_{\mathrm{CE}} = \|C_0 \cdot C_1\|^2 = \| \sum_{i=1}^{K} C_{0,i}^* C_{1,i} \|^2$, where the sum runs over the mode index. We generate a sequence of fake challenge estimates C_1 for which F_{CE} decreases from 1 to 0 and send these challenges through the PUF, keeping the PUF and the setting of SLM2 constant. The corresponding fraction of the light energy in the focus, which is the quantity that determines acceptance or rejection of the key, is shown in Fig. 6.4. We observe $F_{\mathrm{focus}} = \alpha F_{\mathrm{CE}}$, where $\alpha = 0.65 \pm 0.05$ is an experimental factor dominated by the limitation of using a phase-only spatial light modulator. The deviation from linear behavior in the data is periodic in $\sqrt{F_{\mathrm{CE}}}$ and is an experimental artefact caused by periodic noise of the liquid crystal based modulator. The linearity between the challenge estimation fidelity and the fraction of light reaching the focus, as explained in [49], is demonstrated.

6.4.3 Exact physical copy

Another possible attack is to make an exact physical copy of the PUF. For our key this requires positioning millions of particles with the same high refractive index as zinc-oxide and with the correct shapes at the right positions on a 10 nanometer scale. This is not possible with current technology and not likely to become possible in the foreseeable future. To our knowledge no one even tried this. Furthermore, if ever necessary the sensitivity to mispositioning of scatterers can be dramatically increased by choosing alternative PUF designs that enforce much longer pathlengths of light through the scattering medium.

6.4.4 Passive optical device

In principle, a passive optical device could emulate the PUF's physical challenge-response behavior. Since the PUF only realizes a complex linear transformation, one would be tempted to think that it is straightforward to make a passive optical device which does the same optical transformation as the PUF. It is not. The crucial point is that the adversary cannot know which challenge to expect, and therefore can only succeed if his passive optical device produces the correct response for a large fraction of the challenge space. In other words, he will have to emulate a large fraction of the optical properties of the PUF using his optical device. This comes close to making a copy of the PUF. A three-dimensional random scattering medium with front surface area A contains much more random information than can be encoded in a random scattering surface of the same area A. For our sample parameters, a single diffraction-limited spot focused on the surface of the PUF gives rise to a speckle pattern with a Gaussian envelope with a Full Width at Half Maximum (FWHM) of approximately 5μm, containing about 10^2 speckles. When we illuminate the PUF with a random challenge, the illumination spot is much larger than a diffraction-limited spot. The PUF is now seen to reflect a speckle pattern with a FWHM of about 15μm, containing the equivalent of about 10^3 speckles. The reflection matrix describing the PUF is nonlocal (i.e., non-diagonal in e.g. canonical and Fourier representation) as it connects surface points that are spatially separated by up to 5 μm. It is therefore impossible to emulate the PUF with a single scattering surface (e.g., that of an SLM), which would have a local reflection matrix.

Holograms into which a large portion of the PUF's reflection matrix is written can in principle be used to emulate the PUF. Because of the low index of refraction contrast of photorefractive materials, on the order of 0.02 to 0.1 [51], such a hologram must be significantly larger than the true PUF to obtain sufficient reflectivity. Therefore, this form of attack can be easily foiled using a light source with a coherence length of the order of 30 μm, on the order of the average path length photons travel in the PUF. The average optical path in the hologram is much longer than the coherence length so that no speckle pattern will form.

Nanophotonic networks are another candidate for emulating PUFs. Since in principle every passive linear optical network can be emulated by a sufficiently complex network of, e.g., beam splitters [52], this is in theory possible. Work by, e.g., Miller et al. [53, 54] shows the concepts needed to make such a network. However, an adversary who wants to emulate the PUF functionality needs to program a passive optical device with K modes and K^2 connecting elements while keeping all the involved path lengths equal to within the coherence length. Despite the huge efforts already spent in making linear optical networks for linear optical quantum computing and quantum simulation, state of the art networks have at maximum on the order of 50×50 connected beam splitters and losses of 0.2 dB per element for waveguide-based beam splitters [55–58]. Alternative photonic-crystal-based networks could be smaller [59], but the corresponding losses are even higher. In the current QSA implementation 10^3 modes are used. Emulation with a network of beamsplitters requires 10^6 elements. Such a network would have 200 dB loss with current technology [55, 56]. Given the availability of megapixel SLMs it is entirely feasible to extend QSA to use 10^5 modes. Emulation with a network of beamsplitters requires in the order of 10^{10} optical elements and would have a loss of 20000 dB and cover an area of the order of 1m^2 with current technology. In order to make emulation with a network of beamsplitters possible, the overall loss of the network must be 10 dB or less. Therefore, the losses must be reduced to 0.01 dB per element for the current 10^3 mode implementation and to 0.0001 dB per element for the 10^5 mode implementation, while retaining very high phase accuracy and differential path lengths below 30 micrometers. Although there is no law of physics that prevents cloning of the key, this attack is currently technologically infeasible and likely to remain so for at least a decade.

6.4.5 Quantum computer

Only an ideal deterministic quantum computer that can perform arbitrary unitary operations on K-dimensional quantum states of light with low losses would be able to emulate our key. For probabilistic algorithms, which only sometimes give the correct answer, the emulation fidelity averaged over the readout pulses within a single PUF readout is low and therefore they will not work. The most feasible type of quantum-computer for emulation of a PUF seems based on a tunable low-loss K-dimensional optical device. Such a device is at least as difficult to build as a passive low-loss K-dimensional optical device. This is infeasible for the same arguments presented in Section 6.4.4 [60].

6.4.6 Hybrid strategies

An adversary who can create low-loss (i.e. < 10 dB loss) passive optical networks of size $k \times k$ with $k < K$ can use them to create parallel or hybrid systems. The first way he can do this is by placing $\frac{K}{k}$ of these $k \times k$ networks parallel to each other. Each network has a fidelity of $\left(\frac{k}{K}\right)^2$, leading to an overall fidelity of $\frac{k}{K}$. This type of attack is better than a challenge-estimation attack if $\frac{k}{K} > \frac{1}{S+1}$. Another type of parallel system consists of a $k \times k$ passive optical network in parallel with a challenge-estimation attack on the remaining $K - k$ modes. This system has a fidelity of $\left(\frac{k}{K}\right)^2 + \frac{K-k}{K}\frac{1}{S+1}$, which indicates it never works better than either pure challenge-estimation or parallel passive optical networks. With current experimental parameters neither type of hybrid strategy can compete with challenge-estimation attacks. Moreover, like challenge-estimation attacks, parallel systems have an inherently limited fidelity, which allows the verifier to distinguish between the real PUF and a parallel system by choosing an appropriate threshold.

6.4.7 Conclusion regarding attacks against QSA

QSA is insensitive to all types of attacks that we have identified. We expect that if succesful attacks against QSA will be performed, they will most likely be the result of imperfect implementation of QSA and not of flaws in the method itself. This is an important parallel to the field of quantum key distribution. From the analysis in this section we conclude that QSA has a very high potential as a highly secure object authentication method.

6.5 Bringing QSA to the market

QSA appears to have potential to claim a significant role in the global security market. How can this intellectual property [61] be turned into value? We first consider potential commercial partners and then discuss QSA devices we are developing.

6.5.1 Finding early adopters

Commercial parties likely to be interested in QSA can be separated into two categories. On one side there are consumers of authentication solutions, such as banks, governments, hospitals and manufacturers of electronic and other consumer products. There is a large variety of potential consumer applications, and tailoring QSA to the specific demands of one customer may not lead to the best result.

A broader view is obtained by investigating and initiating contact with suppliers of hardware token-based authentication solutions. There are a number of very large authentication companies, including VASCO (e.g. Digipass hardware token), EMC (e.g. SecurID hardware token) and Gemalto. Gemalto is based in the Netherlands and is one of the market leaders, producing e.g. bank cards, SIM cards and electronic passports. These large companies in general do not yet use PUF technology. Their focus seems to be mass production of existing solutions more than pioneering new solutions.

PUF technology is being brought to the market by, typically, smaller companies. Verayo and Intrinsic-ID are leaders in the segment using electronic PUFs for authentication. Their PUFs can be implemented in anything containing a chip, such as modern bank cards and passports. They also specifically target authentication between devices in the rapidly expanding Internet-of-Things (IoT), in which all devices are connected. There is a trend towards user friendly authentication solutions. Many companies such as Apple and Nedap implement near field communication (NFC) for remote authentication. Verayo combines their PUFs with NFC. NXP Semiconductors announced they will implement Intrinsic-ID's PUF technology in their NFC authentication products for additional security. It seems likely more companies will follow suit. The combination of the user-friendly NFC and the security of electronic PUFs seems to be a good benchmark with which to compare QSA.

Two approaches appear viable in bringing QSA to the market:

1. Target applications with the highest security demands: high-cost applications where currently 3-, 4- and 5-factor authentication are used in e.g. government, defense and research,

2. Gain an advantage in applications with medium to high security demands by optimizing the user friendliness of QSA.

The strength of QSA is its very high level of security. The level of acceptance of new technology, such as iris scans, seems highest in the high-end security segment where the stakes are highest. Therefore, the most likely route to succesful valorization of QSA will be to focus initially on the first strategy.

With companies such as Gemalto, NXP Semiconductors, Nedap and Intrinsic-ID we see a strong Dutch representation among leading security companies. This creates opportunities for collaboration and indicates a good local climate for inserting QSA into the global market.

6.5.2 Steps towards a QSA product

As part of the process of bringing QSA to the market we are building a sequence of devices to demonstrate QSA as a secure and practical object authentication method. An overview of these devices and their unique goals and properties is provided here.

1. Proof-of-principle QSA experiment

The first QSA apparatus was built to show the principle of QSA by performing quantum-secure authentication of a key consisting of randomly organized zinc-oxide nanoparticles (see Section 5.2). It used an attenuated diode laser, a liquid crystal-based spatial light modulator and an avalanche photodiode. Readout pulses consist of approximately 230 photons and 1100 spatial modes. A single readout pulse is sufficient for authentication with 10% error rate. 20 readout pulses allow authentication with error rates of 10^{-9}. The experiment was performed in a laboratory environment, which is vibration-free, dark and has a controlled temperature and humidity. The apparatus was large and static, as it was built on an optical table, and it was too slow for practical applications. The key was fixed and vulnerable to heat and humidity fluctuations and other external conditions.

2. Portable wavefront shaping demonstrator

An apparatus was built that demonstrates robustness of wavefront shaping technology in environments with almost no control over vibrations, lighting, temperature and humidity. This apparatus uses a digital micromirror-based spatial light modulator and a CCD camera to focus laser light through random-scattering media (see Fig. 6.5). It works 'out-of-the-box' and even 'out-of-the-car' with no additional alignment requirements and no apparent stability requirements. The speed with which light is shaped is enhanced by an order of magnitude compared to the first experiment by using a digital micromirror device (DMD) instead of a liquid-crystal-based light modulator. The apparatus controls 2500 spatial modes and has a small footprint of 60×60 cm^2.

3. Portable QSA prototype

We are building a portable QSA prototype to demonstrate QSA as a practical and user-friendly object authentication method that is robust to the environment. It is designed to perform QSA in less than 1 second and use a robust key material that is insensitive to temperature and humidity fluctuations. The key will be re-insertable into the QSA device and alignment will be automated. Robustness to misalignment and vibrations may be increased by implementing a small optical element as part of the key. Alignment may be aided by methods developed in our group [62]. Countermeasures against blinding attacks, as described in Section 6.4, will be implemented. The device will have a small footprint ($\ll 1\text{m}^2$) and we are considering cage designs and monolithic designs. This prototype will be

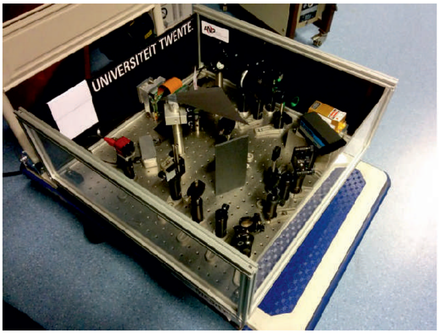


Figure 6.5: Left: portable wavefront shaping demonstrator, right: the author explaining the demonstrator to Dutch vice-minister of education, culture and science Sander Dekker.

accompanied by a 3D animation movie explaining the advantages of QSA when we transport and demonstrate it to potential commercial partners.

6.6 Summary and outlook

Authentication and related security issues are a major concern in modern society. As a result of e.g. software bugs and computer hacks secret information cannot be reliably used for automated authentication of objects and persons. An investigation of possible attack strategies and other object authentication methods shows Quantum-Secure Authentication (QSA) is the most secure practical solution to authentication problems. By providing a secure means of authenticating a key, even if all information about the key is publicly known, QSA mitigates the most pressing problems with current authentication methods. The security market is currently starting to adopt PUF technology and is steadily moving towards more secure solutions that retain a high level of user-friendliness. Considering its extremely high level of security and the remote read-out potential offered by using light, QSA may well be the next step towards a more secure future.

Bibliography

[1] A. Pras, Alle dagen internet - beheersen door beheren, oratierede, 2014. — p.71, 78, 80.

[2] *The internet organised crime threat assessment* (2014), Europol, https://www.europol.europa.eu/sites/default/files/publications/europol_iocta_web.pdf, accessed on February 25, 2015. — p.71, 77.

[3] C. H. Bennett and G. Brassard, *Quantum cryptography: Public key distribution and coin tossing*, IEEE International Conference on Computers, Systems and Signal Processing 175 (1984). — p.71, 75.

[4] R. Maes, *Physically Unclonable Functions: Constructions, Properties and Applications* (Springer-Verlag Berlin Heidelberg, Germany, 2013). — p.73.

[5] R. Pappu, B. Recht, J. Taylor, and N. Gershenfeld, *Physical one-way functions*, Science **297**, 2026 (2002). — p.73.

[6] S. J. Wiesner, *Conjugate coding*, ACM SIGACT News **15**, 78 (1983). — p.73.

[7] F. Pastawskia, N. Y. Yaob, L. Jiang, M. D. Lukinb, and J. I. Cirac, *Unforgeable noise-tolerant quantum tokens*, Proc. Natl. Acad. Sci. U.S.A. **109**, 16079 (2012). — p.73.

[8] S. Wehner, C. Schaffner, and B. M. Terhal, *Cryptography from noisy storage*, Phys. Rev. Lett. **100**, 220502 (2008). — p.73.

[9] C. Paar and J. Pelzl, *Understanding cryptography* (Springer Berlin Heidelberg, 2010), pp. 319–330. — p.74.

[10] R. Rivest, A. Shamir, and L. Adleman, *A method for obtaining digital signatures and public-key cryptosystems*, Commun. ACM **21**, 120 (1978). — p.74.

[11] R. J. McEliece, *A public-key cryptosystem based on algebraic coding theory*, Deep Space Network Progress Report **42-44**, 114 (1978). — p.74.

[12] W. Diffie and M. E. Hellman, *New directions in cryptography*, IEEE Trans. Inf. Theory **IT-22**, 644 (1976). — p.74.

[13] V. Scarani, A. Acín, G. Ribordy, and N. Gisin, *Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations*, Phys. Rev. Lett. **92**, 057901 (2004). — p.75.

[14] *Multi-factor authentication market worth \$10.75 billion by 2020* (2014), MarketsandMarkets, http://www.marketsandmarkets.com/PressReleases/multi-factor-authentication.asp, accessed on February 25, 2015. — p.76.

[15] *Global multi-factor authentication market 2014-2018* (2014), Technavio, http://www.technavio.com/report/global-multi-factor-authentication-market-2014-2018, accessed on February 25, 2015. — p.76.

[16] S. W. Inscoe, *Global consumers react to rising fraud: beware back of wallet* (2012), Aite Group LLC, http://www.aciworldwide.com/ /media/files/collateral/aci_aite_global_consumers_react_to_rising_fraud_1012, accessed on February 25, 2015. — p.76.

[17] *Global card fraud losses reach \$11.27 billion* (2013), The Nilson Report, http://www.nilsonreport.com/publication_chart_and_graphs_archive.php?1=1&year=2013, accessed on February 25, 2015. — p.76.

[18] B. Krebs, *All about skimmers* (2010-2014), Krebs on Security, http://krebsonsecurity.com/all-about-skimmers/, accessed on February 25, 2015. — p.77.

[19] S. Gold, *The evolution of payment card fraud*, Computer Fraud & Security 12 (2014). — p.77, 78.

[20] B. Krebs, *Cards stolen in Target breach flood underground markets* (December 13, 2013), Krebs on Security, http://krebsonsecurity.com/2013/12/cards-stolen-in-target-breach-flood-underground-markets/, accessed on February 25, 2015. — p.77.

[21] B. Krebs, *Coordinated ATM heist nets thieves \$13M* (August 11, 2011),

Krebs on Security, http://krebsonsecurity.com/2011/08/coordinated-atm-heist-nets-thieves-13m/, accessed on February 25, 2015. — p.78.

[22] M. Bond, O. Choudary, S. J. Murdoch, S. Skorobogatov, and R. Anderson, *Chip and skim: cloning EMV cards with the pre-play attack*, arXiv:1209.2531 (2012). — p.78.

[23] J. Scahill and J. Begley, *The great SIM heist* (February 19, 2015), The Intercept, https://firstlook.org/theintercept/2015/02/19/great-sim-heist/, accessed on March 9, 2015. — p.78, 80.

[24] N. Vinocur and E. Auchard, *SIM maker Gemalto says spies probably did hack it but plays down impact* (February 25, 2015), reuters, http://www.reuters.com/article/2015/02/25/us-gemalto-cyberattack-idUSKBN0LT0MW20150225, accessed on March 9, 2015. — p.78, 80.

[25] C. Helfmeier, D. Nedospasov, C. Tarnovsky, J. Krissler, C. Boit, and J.-P. Seifert, *Breaking and entering through the silicon,* in CCS '13 proceedings of the 2013 ACM SIGSAC conference on computer & communications security, 733 (2013). — p.78.

[26] D. Everett, *What the silicon manufacturer has put together let no man put asunder* (2010), http://www.microexpert.com/assets/pdfs/What%20the%20silicon%20manufacturer%20has%20put%20together%20let%20no%20man.pdf, accessed on March 9, 2015. — p.78.

[27] By FenixFeather (Inkscape) [CC BY-SA 3.0 (http://creativecommons.org/licenses/by-sa/3.0)], via Wikimedia Commons. — p.79.

[28] Z. Durumeric, J. Kasten, D. Adrian, J. A. Halderman, M. Bailey, F. Li, N. Weaver, J. Amann, J. Beekman, M. Payer, and V. Paxson, *The matter of Heartbleed*, IMC '14 Proceedings of the 2014 conference on internet measurement conference 475 (2014). — p.78.

[29] T. Hunt, *Everything you need to know about the Heartbleed SSL bug* (April 9, 2014), http://www.troyhunt.com/2014/04/everything-you-need-to-know-about.html, accessed on February 25, 2015. — p.78.

[30] P. Mutton, *Half a million widely trusted websites vulnerable to Heartbleed bug* (2014), Netcraft, http://news.netcraft.com/archives/2014/04/08/half-a-million-widely-trusted-websites-vulnerable-to-heartbleed-bug.html, accessed on February 25, 2015. — p.78.

[31] J. Sigholm, *Determining the utility of cyber vulnerability implantation: The Heartbleed bug as a cyber operation*, IEEE MILCOM 110 (2014). — p.79.

[32] S. M. Kerner, *Heartbleed SSL flaw's true cost will take time to tally* (April 19, 2014), eWeek, http://www.eweek.com/security/heartbleed-ssl-flaws-true-cost-will-take-time-to-tally.html, accessed on February 25, 2015. — p.79.

[33] S. Mansfield-Devine, *Hacking on an industrial scale*, Network Security 12 (2014). — p.79.

[34] J. Verble, *The NSA and Edward Snowden: surveillance in the 21st century*, ACM SIGCAS Computers and Society **44**, 14 (2014). — p.80.

[35] NSA, https://www.nsa.gov/, accessed on February 25, 2015, — p.80.

[36] M. Riley, *NSA said to have used Heartbleed bug, exposing consumers* (2014),

BloombergBusiness, http://www.bloomberg.com/news/articles/2014-04-11/nsa-said-to-have-used-heartbleed-bug-exposing-consumers, accessed on February 25, 2015. — p.80.

[37] J. Menn, *Exclusive: Secret contract tied NSA and security industry pioneer* (December 20, 2013), Reuters, http://www.reuters.com/article/2013/12/20/us-usa-security-rsa-idUSBRE9BJ1C220131220, accessed on February 25, 2015. — p.80.

[38] *IFIP statement on intentional weakening of security and trust mechanisms in ICT and the internet by government agencies and other major actors* (October 24, 2013), International Federation for Information Processing, http://www.gi.de/fileadmin/redaktion/Download/web_ifip_statement_underminingsecuritytrust_mechanisms_4_0.unanimously.pdf, accessed on February 25, 2015. — p.80.

[39] L. Levison, *Open letter* (August 8, 2013), http://lavabit.com/, accessed on February 25, 2015. — p.80.

[40] L. Levison, *Open letter* (May 20, 2014), http://lavabit.com/, accessed on February 25, 2015. — p.80.

[41] G. Greenwald and E. MacAskill, *NSA Prism program taps in to user data of Apple, Google and others* (June 7, 2013), The Guardian, http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data, accessed on February 25, 2015. — p.80.

[42] J. Ball, *NSA's Prism surveillance program: how it works and what it can do* (June 8, 2013), The Guardian, http://www.theguardian.com/world/2013/jun/08/nsa-prism-server-collection-facebook-google, accessed on February 25, 2015. — p.80.

[43] N. Perlroth, J. Larson, and S. Shane, *N.S.A. able to foil basic safeguards of privacy on web* (September 5, 2013), The New York Times, http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html?pagewanted=3&_r=2, accessed on February 25, 2015. — p.80.

[44] R. Gallagher and G. Greenwald, *How the NSA plans to infect millions of computers with malware* (March 12, 2014), The Intercept, https://firstlook.org/theintercept/2014/03/12/nsa-plans-infect-millions-computers-malware/, accessed on February 25, 2015. — p.81.

[45] *NSA phishing tactics and man in the middle attacks* (March 12, 2014), The Intercept, https://firstlook.org/theintercept/document/2014/03/12/nsa-phishing-tactics-man-middle-attacks/, accessed on February 25, 2015. — p.81.

[46] *Five eyes hacking large routers* (March 12, 2014), The Intercept, https://firstlook.org/theintercept/document/2014/03/12/five-eyes-hacking-large-routers/, accessed on February 25, 2015. — p.81.

[47] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, *Hacking commercial quantum cryptography systems by tailored bright illumination*, Nature Photon. **4**, 686 (2010). — p.81.

[48] B. Škorić, *Quantum readout of physical unclonable functions*, Int. J. Quant. Inf. **10**, 1250001 (2012). — p.82.

[49] B. Škorić, A. P. Mosk, and P. W. H. Pinkse, *Security of quantum-readout PUFs against quadrature-based challenge-estimation attacks*, Int. J. Quant. Inf. **11**, 1350041 (2013). — p.82, 83.

[50] B. Škorić, *Security analysis of quantum-readout PUFs in the case of challenge-estimation attacks*, submitted, http://eprint.iacr.org/2013/479 (2013). — p.82.

[51] S. C. Barden, J. A. Arns, and W. S. Colburn, *Volume-phase holographic gratings and their potential for astronomical applications*, Proc. SPIE **3355**, 866 (1998). — p.84.

[52] M. Reck, A. Zeilinger, H. J. Bernstein, and P. Bertani, *Experimental realization of any discrete unitary operator*, Phys. Rev. Lett. **73**, 58 (1994). — p.84.

[53] D. A. B. Miller, *All linear optical devices are mode converters*, Opt. Express **20**, 23985 (2012). — p.84.

[54] D. A. B. Miller, *Self-configuring universal linear optical component*, Photon. Res. **1**, 1 (2013). — p.84.

[55] S. Han, T. J. Seok, N. Quack, B.-W. Yoo, and M. C. Wu, *Monolithic 50x50 MEMS silicon photonic switches with microsecond response time* in Optical Fiber Communication Conference (Optical Society of America, 2014). — p.84.

[56] D. D. John, M. J. R. Heck, J. F. Bauters, R. Moreira, J. S. Barton, J. E. Bowers, and D. J. Blumenthal, *Multilayer platform for ultra-low-loss waveguide applications*, IEEE Photon. Technol. Lett. **24**, 876 (2012). — p.84.

[57] P. J. Shadbolt, M. R. Verde, A. Peruzzo, A. Politi, A. Laing, M. Lobino, J. C. F. Matthews, M. G. Thompson, and J. L. O'Brien, *Generating, manipulating and measuring entanglement and mixture with a reconfigurable photonic circuit*, Nature Photon. **6**, 45 (2011). — p.84.

[58] J. Sun, E. Timurdogan, A. Yaacobi, E. S. Hosseini, and M. R. Watts, *Large-scale nanophotonic phased array*, Nature **493**, 195 (2013). — p.84.

[59] Y. Jiao, S. Fan, and D. A. B. Miller, *Demonstration of systematic photonic crystal device design and optimization by low-rank adjustments: an extremely compact mode separator*, Opt. Lett. **30**, 141 (2005). — p.84.

[60] D. P. DiVincenzo, *Towards control of large-scale quantum computing*, Science **334**, 50 (2011). — p.85.

[61] P. W. H. Pinkse, A. P. Mosk, and B. Škorić, *Quantum secure device, system and method for verifying challenge-response pairs using a physically unclonable function (PUF)*, European Patent EP2693685 A1 (also published as WO2014019678 A1) (February 5, 2014). — p.85.

[62] E. G. van Putten, A. Lagendijk, and A. Mosk, *Non-imaging speckle interferometry for high speed nanometer-scale position detection*, Opt. Lett. **37**, 1070 (2012). — p.87.

CHAPTER 7

Summary

In this thesis we explore the use of shaped wavefronts for elucidating the fundamental physics of wave scattering and for applications in security. One important phenomenon particular to wave scattering is the occurrence of open channels, which fully transmit light through a thick scattering sample. Long-lived modes are an even more intriguing phenomenon, where light remains trapped inside the sample for a much longer time than predicted by diffusion theory. Finally, we investigate and exploit the combination of multiple-scattering of light with quantum physics, which provides a unique mixture of highly desirable properties when applied to authentication of objects.

In Chapter 2 methods for efficiently addressing open channels and long-lived modes are investigated. Open channels can be purified by iteratively phase conjugating the light field transmitted through a multiple-scattering slab. We propose to purify long-lived modes using a similar procedure: iterative phase conjugation of the frequency-derivative of the transmitted field. Numerical simulations predict that the efficiency with which light will be coupled to open channels and long-lived modes is approximately equal to the phase conjugation fidelity F of the experimental apparatus. Therefore, efficient coupling to open channels and long-lived modes is likely within experimental reach. The next two chapters are concerned with creating the necessary conditions for their observation.

In Chapter 3 a superpixel method for accurate and high-resolution control over the light field is proposed and experimentally demonstrated. We group pixels of a digital micromirror device (DMD) into superpixels of, typically, 4×4 pixels. After low-pass filtering, the light diffracted from a superpixel under a small angle is accurately controlled in phase and intensity. Measured and calculated modulation fidelities exceed that of state-of-the-art Lee holography, while our method is equally light efficient and robust to misalignment. Therefore, the superpixel method is an excellent tool for controlling propagation of light in multiple-scattering media.

In Chapter 4 an apparatus is described that we designed and built, aiming at an unparalleled level of control over light in multiple-scattering media. The apparatus consists of vector field synthesizers and detectors that control and detect the light field on both sides of a multiple-scattering slab simultaneously and independently in approximately 100×100 effective pixels. The light source is a frequency-tunable CW laser which can resolve a broad range of mode lifetimes of approximately 130 fs up to 0.2 ns. The phase conjugation fidelity is designed to be $F > 0.5$. It is, therefore, expected that the apparatus can achieve record-high transmission through optically thick media and is an excellent candidate for making the first-ever observation of long-lived modes for light in 3D disordered media. The apparatus can also be used for cryptography in multiple-scattering media.

In Chapter 5 we experimentally demonstrate quantum-secure authentication (QSA) of a physical unclonable key, a method to securely authenticate objects. The key is a multiple-scattering medium and cannot be copied due to limitations of modern and foreseeable technology. An adversary also cannot use digital devices to measure the incident light wave and produce the correct response speckle pattern, because of the quantum nature of light. Moreover, QSA does not depend on unproven mathematical assumptions and is relatively straightforward to implement. We experimentally demonstrate QSA and argue it is the most secure practical object authentication method currently available.

In Chapter 6 the potential importance of QSA for society is investigated. A comparison to other authentication methods reveals that the security against copying as well as digital emulation is unique among currently available object authentication methods. QSA is the most secure practical method when all information about the key is publicly known. An investigation of recent authentication-based security breaches shows that this is highly relevant, as authentication information is notoriously difficult to protect and leakage of authentication information is the main cause of security breaches. In-depth analysis of potential attacks against QSA shows that all attacks we analyzed fail or can be easily prevented. Finally, we observe that the authentication market is moving towards more-secure authentication primitives while maintaining a high level of user-friendliness. Considering its very high level of security combined with the remote-readout potential offered by using light, QSA may take a leading position in this trend.

The methods described in this thesis contribute to the rapidly growing field of controlling light in multiple-scattering media. We demonstrate a new method for controlling light and set the stage for further investigation of open channels and long-lived modes. Finally, multiple light scattering combined with quantum physics finds an intriguing application in secure authentication.

Nederlandse samenvatting

In materialen zoals papier, eiwit en huid wordt licht verstrooid. Lichtverstrooiing is een interessant fenomeen vanuit fundamenteel oogpunt en is van groot praktisch belang, bijvoorbeeld in de gezondheidszorg, voor sensoren en microscopen, in de beveiliging en wellicht ook voor efficiëntere zonnecellen en LEDs. In dit proefschrift onderzoeken we het gebruik van geprepareerde golffronten voor twee doeleinden, namelijk om beter inzicht te krijgen in fundamentele fysica op het gebied van golfverstrooiing en voor toepassingen in de beveiliging. Een belangrijk verschijnsel is het optreden van open kanalen, die ervoor zorgen dat licht volledig doorgelaten kan worden door sterk verstrooiende lagen zoals papier en de huid. Nog intrigerender zijn langlevende toestanden, waarbij licht veel langer dan gemiddeld opgesloten blijft in zo'n verstrooiend materiaal. Tot slot onderzoeken en benutten we de combinatie van meervoudige lichtverstrooiing met kwantumfysica, waaruit een unieke combinatie van zeer wenselijke eigenschappen voortvloeit voor authenticatie van voorwerpen zoals bankpassen en paspoorten.

In hoofdstuk 2 worden methoden voor het efficiënt koppelen van licht aan open kanalen en langlevende toestanden theoretisch onderzocht. Efficiënte koppeling aan open kanalen kan bereikt worden door middel van herhaaldelijke fase conjugatie van het lichtveld dat door een meervoudig verstrooiende laag doorgelaten wordt. Wij stellen een vergelijkbare procedure voor om licht aan langlevende toestanden te koppelen: herhaaldelijke fase conjugatie van de frequentie-afgeleide van het doorgelaten lichtveld. Numerieke simulaties voorspellen dat de efficiëntie waarmee licht aan open kanalen en langlevende toestanden gekoppeld kan worden ongeveer gelijk is aan de fase conjugatie precisie F van het experimentele apparaat. Het efficiënt koppelen aan open kanalen en langlevende toestanden lijkt dan ook experimenteel haalbaar. De volgende twee hoofdstukken gaan over het creëren van de benodigde randvoorwaarden om open kanalen en langlevende toestanden te observeren.

In hoofdstuk 3 wordt een superpixelmethode voorgesteld en experimenteel gedemonstreerd om nauwkeurig en met hoge resolutie lichtvelden te vormen. We groeperen pixels van een digitaal microspiegel apparaat (DMD) tot superpixels van, meestal, 4×4 pixels. Na diffractie van een superpixel onder een kleine hoek en middeling van het lichtveld over een superpixel worden zowel de intensiteit als de fase van het lichtveld nauwkeurig geregeld. De gemeten en berekende precisie is hoger dan die van state-of-the-art Lee holografie, terwijl onze methode een even hoge lichtefficiëntie heeft en even robuust is ten aanzien van uitlijnfouten. Daardoor vormt de superpixelmethode een uitstekend hulpmiddel voor het manipuleren van de voortplanting van licht in verstrooiende materialen.

In hoofdstuk 4 wordt een apparaat beschreven dat we ontworpen en gebouwd hebben met als doel een ongeëvenaard niveau van controle over licht in meervoudig verstrooiende materialen te bereiken. Het apparaat bestaat uit golffront vormers en detectoren die het lichtveld vormen en meten aan beide kanten van een meervoudig verstrooiende laag in ongeveer 100×100 onafhankelijke effectieve pixels. De lichtbron is een monochromatische laser waarvan de frequentie verstemd kan worden, zodat we een groot bereik van levensduren kunnen onderzoeken van ongeveer 130 femtoseconden tot 0,2 nanoseconden. Het ontwerp maakt een fase conjugatie precisie van $F > 0{,}5$ mogelijk. Daardoor verwachten we dat het apparaat zeer hoge transmissie door een optisch dik materiaal kan bereiken en uitermate geschikt is om voor het eerst langlevende toestanden van licht in 3D wanordelijke materialen aan te tonen. Het apparaat kan ook gebruikt worden voor cryptografie in meervoudig verstrooiende materialen.

In hoofdstuk 5 hebben we kwantum-veilige authenticatie (QSA) met een fysiek onkloonbare sleutel experimenteel gedemonstreerd. QSA is een methode om voorwerpen veilig te authenticeren. De sleutel is een meervoudig verstrooiend materiaal en kan niet gekopieerd worden vanwege de limieten van de huidige technologie. Dankzij kwantumeigenschappen van licht kan een tegenstander ook geen digitale apparatuur gebruiken om het inkomende lichtveld te meten en het verwachte antwoord te produceren. Bovendien is QSA niet gebaseerd op wiskundige aannames die niet bewezen zijn en is het relatief eenvoudig te implementeren. Wij hebben QSA experimenteel gedemonstreerd en beargumenteren dat het de meest veilige praktische authenticatiemethode voor voorwerpen is die momenteel beschikbaar is.

In hoofdstuk 6 wordt het potentieel belang van QSA voor de samenleving onderzocht. Een vergelijking met andere authenticatiemethoden laat zien dat de veiligheid tegen zowel kopiëren als digitale emulatie uniek is onder beschikbare authenticatiemethoden voor voorwerpen. QSA is de enige praktische methode die veilig is zelfs als alle informatie over de sleutel publiek toegankelijk is. Onderzoek naar recente beveiligingsproblemen gebaseerd op authenticatie laat zien dat dit hoogst relevant is, aangezien authenticatie-informatie notoir moeilijk te beschermen is en lekkage van authenticatie-informatie de belangrijkste oorzaak van inbreuken op de beveiliging is. Een grondige analyse van de mogelijke aanvallen op QSA toont aan dat alle aanvallen die we geanalyseerd hebben mislukken of gemakkelijk te voorkomen zijn. Tot slot zien we dat authenticatiemarkt verschuift naar veiligere authenticatiemethoden met behoud van een hoge mate van gebruiksvriendelijkheid. Gezien het zeer hoge niveau van veiligheid in combinatie met de mogelijkheid om sleutels op afstand uit te lezen zou QSA een leidende positie in kunnen gaan nemen in deze trend.

De in dit proefschrift beschreven methoden dragen bij aan het snelgroeiende onderzoeksveld waarin de voortplanting van licht door meervoudig verstrooiend materiaal gemanipuleerd wordt. Wij hebben een nieuwe methode voor het vormen van lichtvelden gedemonstreerd en hebben de weg geëffend voor verder onderzoek naar open kanalen en langlevende toestanden. Tot slot heeft de combinatie van meervoudige lichtverstrooiing met kwantumfysica tot een intrigerende toepassing geleid in veilige authenticatie.

Acknowledgements

During the last four years I grew from a young mathematician who barely knew that light is a wave to the experimental physicist who is writing this thesis. An extremely diverse group of people contributed to this process, all of whom I am very grateful.

Allereerst wil ik mijn ouders, Jan en Dina Goorden, bedanken voor hun schijnbaar onbegrensde steun en vertrouwen. Samen met mijn zusje Loes, met wie ik een bijzonder sterke band heb, bieden zij de basis die me hier heeft gebracht.

A pivotal role was played by Wilbert IJzerman and Teus Tukker. Besides their excellent guidance during my master project, they recognized a physicist in me and introduced me to the Complex Photonic Systems (COPS) group.

The first COPS I remember meeting is our group leader Willem Vos. His passion for educating people on a scientific as well as personal level makes COPS the exceptionally good learning environment that it is and is one of the reasons I joined. My advisor Allard taught me most of the things I learned during my PhD. I think he is best known for his incredible knowledge, but he is also a great coach for whom the development of his students is the top priority. From my advisor Pepijn I learned a lot about science as well as about other aspects of life. His enthusiasm is inspiring and I appreciate the balance he brings to COPS. Our collaborator Boris Škorić proposed QSA. His knowledge about cryptography and his push towards more precise formulations were crucial during my PhD. I was very lucky to work with Ad Lagendijk and learn about his strong and clearly expressed ideas on science, doing science and life.

Group technician Cock Harteveld helped me out many times, in particular when I had experimental questions. I am very grateful to secretaries Nilda Rijpma and Nienke Timmer for resolving many administrative issues. Whenever I had computer problems, Marlon Gomperts was very quick to fix them. Their value for running an efficient scientific group can, in my opinion, not be overestimated.

During the first year of my PhD I worked closely together with fellow PhD student Marcel Horstmann. Besides a great guy he is perhaps the most practical and efficient of everyone I worked with. He built a large part of the QSA apparatus and showed me that the fastest solution that gets the job done is often the best. In terms of getting me up to speed with optics, our former postdoc Jacopo Bertolotti was perhaps most important of everyone I worked with. I will never forget how patiently he answered our infinite stream of questions. Hasan Yılmaz, famous for his enthusiasm and laugh, started his PhD just before me. I couldn't hope for a better friend to share this experience with. Only he would spend two days with me to understand (spatial) coherence and how to exploit it, while others are wondering why we are not working. I learned about transmission matrices from Duygu Akbulut, who was finishing her experiments when I joined. We had many interesting discussions during dinner and tea breaks in those busy evenings. Soon after he joined, postdoc and friend Henri Thyrrestrup became very important for COPS and for me. He can very often be found discussing other people's projects with them. He tends to enter my office at exactly the right time, not rarely ending up there the whole evening helping me out with some software or other problem. Diana Grishina gained a special place in my life with her amazing mixture of energy, emotion and honesty. Every day with her is colorful.

I'd like to thank Jin Lian for being such a sharp observer of important as well as unimportant matters and for being a very nice and curious friend and colleague. My mathematician office mate, sexiest Indian colleague and friend Devashish, who never says a bad word about anyone, was a great support. Andreas Schulz and Emre Yüce are good friends and always ready to give advice. I appreciate Simon Huisman's efforts to keep COPS sharp and professional and to make me go home in the evenings. Tom Wolterink helped me greatly building up experiments during the last years and is equally great for having a casual chat. Núria Taberner Carretero designed our beautiful Optica cover image. Other valuable contributions were made by Adrien, Amandev, Bergin, Bill, David, Dirk-Jan, Elahe, Elbert, Evangelos, Femi, Georgios, Ivo, Jan, Jean, Jeffrey, Jennifer, Jochen, Jorge, Kasper, Klaas-Jan, Klaus, Kurt, Lyuba, Maryna, Mike, Muharrem, Naser, Peter, Raheleh, Ramy, Ravitej, Recep, Reinier, Rik, Rob, Sergei, Sina, Thomas Huisman, Thomas Hummel, Timmo, Tristan, Vanessa, Willem Tjerkstra, Yin, Yonatan and Youwen.

It was a pleasure advising bachelor students Guus Spenkeling and Melanie Peters and the excellent summer student Michael (Vandy) Van De Graaff. I am very happy to work with the talented Jeroen Bosch who is continuing my experiments during his master project.

Besides my friends in Enschede, mentioned above, I thank my friends elsewhere, in particular around Eindhoven and around Schijf. After weeks of hard work it is always a lot of fun and very refreshing to meet you all again.

- Bas