RESPONSE TO REFEREES

We appreciate the referees’ comments and suggestions, and we have modified our manuscript in accordance with the referee reports. Below we respond to all of the referee's concerns in detail.

The referee report is reproduced verbatim and in full below as indented blue Times New Roman font, and our point-by-point responses are in non-indented black Helvetica font. In addition to these changes, we have made minor edits to improve the readability of the manuscript.

Changes to the manuscript appear in the revised manuscript in red font.

**Review 1:**

A REPORT ON:

"The resurgence of the linear optics interferometer — recent

advances & applications"

BY

Si-Hui Tan and Peter P. Rohde

===

It is a relatively short but comprehensive review on recent applications of linear-optical interferometers to quantum information processing and quantum engineering. These interferometers include the Mach-Zehnder interferometer and its multiport generalizations.

It is an interesting, up-to-date, and sound review having a logical and consistent structure. I have enjoyed reading this manuscript.

Thus, I could recommend the manuscript for publication in "Reviews in Physics".

I would only suggest the authors to mention some other closely-related topics (including, e.g., quantum simulations, quantum key distribution based on interferometers, or optimal quantum cloning also based on interferometers), as I list below.

I understand that the literature on quantum-information applications of quantum-optical interferometers is overwhelming, so it is a matter of personal choice to cite some of these articles and ignore the vast majority. Anyway, this review cites

only 126 references. Quite often regular articles (published in, e.g., PRA) have a similar number of references. Thus, I would also suggest to cite more relevant papers.

We thank the referee for the positive review, and for his suggestions for additional topics to include in our review. It is our aim to be as interesting and relevant to a broad readership as possible. As such, we have tried to include as many as we could of the above suggested topics. Partly based on his suggestions, we have added new sections on (1) quantum state and process tomography (Sec. 6), (2) quantum state engineering based on the multi-port Mach-Zehnder interferometer (Sec. 7.6), (3) optical switch (Sec. 10), (4) quantum simulations (Sec. 11.3), (5) repeater networks (Sec. 11.5). We have also added a paragraph on quantum key distribution under subsection 11.1, and on other sampling problems in subsection 11.2.

Here are my detailed comments:

%------------------------------------------------------------------

(1) It is written in the Introduction that:

> "In 2001, Knill, Laflamme and Milburn (KLM) showed that efficient

> quantum computing is possible using only linear optical

> components, that is single photons, beamsplitters, phase shifters

> and photon counting [3]"

Note that "efficient quantum computing ... using only linear optical components" has been independently introduced by:

> M. Koashi, T. Yamamoto, and N. Imoto,

> Probabilistic manipulation of entangled photons,

> Physical Review A 63, 030301(R) (2001).

This reference was published on 12 February 2001, while [3] was published on 4 January 2001, so almost simultaneously.

We thank the referee for pointing out the missed reference. We have revised our introduction to:

“In 2001, Knill, Laflamme and Milburn (KLM) showed that efficient quantum computing is possible using only linear optical components, that is single photons, beamsplitters, phase shifters and photon counting for spatially encoded qubits [3]. At about the same time, Koashi, Yamamoto, and Imoto (KYI) essentially came to the same result for polarization-encoded qubits [4].”

In the above revision, [4] is the missing reference by Koashi, Yamamoto, and Imoto.

(2) Surprisingly, the field of quantum simulation in not mentioned in this review at all. However, boson sampling has been often discussed in relation to classical and quantum simulations.

For example,

> Diego G. Olivares, Borja Peropadre, Alán Aspuru-Guzik, Juan José García-Ripoll

> Quantum Simulation with a Boson Sampling Circuit

> Phys. Rev. A 94, 022319 (2016)

Also efficient classical simulation of linear-quantum optics was discussed in

> S. Rahimi-Keshari, T. C. Ralph, C. M. Caves

> Sufficient Conditions for Efficient Classical Simulation of Quantum Optics

> Phys. Rev. X 6, 021039 (2016)

Reviews on quantum simulation include:

> I. Buluta, F. Nori,

> Quantum Simulators,

> Science 326, 108-111 (2009).

>

> I. Georgescu, S. Ashhab, F. Nori,

> Quantum Simulation,

> Rev. Mod. Phys. 86, 153 (2014).

We thank the referee for pointing out our oversight. We have added a new section, Sec. 10.4, to discuss quantum simulations.

(3) Quantum key distribution (QKD) is mentioned \*only\* in the Introduction as follows:

> "Photons make fantastic ‘flying’ qubits, and are readily used for

> quantum communication [1] and quantum key distribution [2]"

QKD for secure quantum communication is one of a very few commercial applications of quantum optics. So, this topic deserves to be shortly discussed in this review. This might be combined with quantum computation in Sec. 9.1.

For example,

(3.1) the B92 protocol is a standard example of quantum key distribution, which can be based on Mach-Zehnder interferometer, as introduced and described by:

> C. H. Bennett,

> Quantum cryptography using any two nonorthogonal states,

> Phys. Rev. Lett. 68, 3121 (1992)

The B92 protocol has been experimentally implemented as reported, e.g.,

> R. J. Hughes, G. L. Morgan, C. G. Peterson,

> Practical quantum key distribution over a 48-km optical fiber network,

> Journal of Modern Optics 47 (2000).

(3.2) A recent sound proposal of a QKD protocol by:

> T. Sasaki, Y. Yamamoto, M. Koashi

> Practical quantum key distribution protocol without monitoring signal disturbance

> Nature 509, 475–478 (2014)

also uses the Mach-Zehnder interferometer (on Bob's site.)

Note that this QKD has also been experimentally implemented:

> H. Takesue, T. Sasaki, K. Tamaki, and M. Koashi

> Experimental quantum key distribution without monitoring signal disturbance

> Nature Photonics 9, 827–831 (2015)

(3.3) Moreover, entanglement-based quantum key distribution based

on the Franson interferometer:

> J.D. Franson,

> Bell Inequality for Position and Time,

> Phys. Rev. Lett. 62, 2205 (1989).

has been attracting some interest, see, e.g.:

> T. Brougham et al.

> Security of high-dimensional quantum key distribution protocols using Franson interferometers

> J. Phys. B: At. Mol. Opt. Phys. 46 (2013) 104010.

> I. Ali-Khan, C. J. Broadbent, and J. C. Howell,

> Large-Alphabet Quantum Key Distribution Using Energy-Time Entangled Bipartite States,

> PRL 98, 060503 (2007)

We had not included QKD in the review originally because quantum interferometry is not strictly needed for QKD. However, we agree that it is an active area of research, and that it would be relevant for readers if we discuss it here. For this, we have added a paragraph in Sec. 11.1. While considering QKD, we have also added a related section, Sec. 11.5, on quantum repeater networks.

(4) Quantum engineering based on the multi-port Mach-Zehnder interferometer of Reck et al. [31] has also attracted some interest.

For example, quantum teleportation, state truncation (linear photon-blockade), and hole burning in Fock space using this interferometer were discussed by:

> A. Miranowicz et al.,

> Selective truncations of an optical state using projection synthesis,

> J. Opt. Soc. Am. B 24, 379-383 (2007)

We have added a new section, Sec. 7.6, to discuss quantum engineering based on the multi-port Mach-Zehnder interferometer.

(5) Optimal quantum-optical cloning implementations are also based on (lossy) Mach-Zehnder interferometers (referred to as a beam divider assembly). These cloners were applied, e.g., for the eavesdropping of realistic QKD systems and the forgery of quantum money by, e.g.:

> K. Bartkiewicz et al.,

> Experimental quantum forgery of quantum optical money,

> npj Quantum Information 7 (3) 1 (2017).

> H. Fan et al.,

> Quantum Cloning Machines and the Applications,

> Phys. Rep. 544, 241 (2014).

> K. Bartkiewicz et al.,

> Experimental eavesdropping based on optimal quantum cloning,

> Phys. Rev. Lett. 110, 173601 (2013).

Based on the referee’s recommendation, we have included a mention of quantum optical implementations of quantum cloning, and its application to attacks on quantum cryptographic schemes at the end of Sec. 11.1 immediately following the new part describing QKD.

(6) LIGO experiment based on Michelson interferometer can be mentioned in one sentence in the Introduction:

> B.P. Abbott et al.,

> Observation of Gravitational Waves from a Binary Black Hole Merger,

> Phys. Rev. Lett. 116, 061102 (2016)

The LIGO experiments are now mentioned and cited at the beginning of the second paragraph of the introduction.

(7) There are various linear-optical implementations of two-qubit

gates. A list of 30 such implementations of CS/CNOT gates is presented in:

> M. Bartkowiak and A. Miranowicz,

> Linear-optical implementations of the iSWAP and controlled NOT gates based on conventional detectors,

> J. Opt. Soc. Am. B 27, 2369-2377 (2010)

The reference to the above paper is now included at the beginning of Section 11.1 as Ref. [122] in the following sentence: “Various linear-optical implementations of two-qubit gates important for approximately universal quantum computation are listed in Ref. [122], …”

(8) A note can be added to the caption of Fig. 1, that the setup describes a generalized multi-port Mach-Zehnder interferometer.

We have added the following sentence to the caption of Fig. 1: “This setup describes a generalized multi-port Mach-Zehnder interferometer.”

(9) In order to describe more realistic (imperfect) photon-number detectors, it can be mentioned in Sec. 8 that positive-operator-valued measures (POVMs) should be used to describe the effects of detector finite efficiency, finite-number resolution, and dark counts. Such POVMs are discussed in, e.g.:

> S. M. Barnett, L. S. Phillips, and D. T. Pegg,

> Imperfect photodetection as projection onto mixed states,

> Opt. Commun. 158, 45 (1998).

>

> S. Ozdemir et al.,

> Quantum-scissors device for optical state truncation: A proposal for practical realization,

> Phys. Rev. A 64, 063818 (2001).

We have added a paragraph following eq. (15) to describe the representation of photodetector outcomes when realistic effects are considered. The above mentioned works have been cited, among others.

(10) The following relevant book can be cited:

> P. Kok and B. W. Lovett,

> Introduction to Optical Quantum Information Processing,

> Cambridge Univ. Press, 2010

We have added a citation to Kok and Lovett at the end of the first sentence in the introduction.

Minor comments:

(11) There are typos in the titles of a few references, e.g.,

[13,24,32,79,107,112]

The typos in the above titles have been corrected. There were also formatting issues for some references, and these have been cleaned up.

(12) Please correct the spelling of Zehnder in the phrase

"Mach-\*Zedner\* interferometer" in two places.

The misspellings for “Zehnder” have been found and corrected.

**Review 2:**

This review provides up-to-date summary on the applications of linear optical couplers and interferometers for implementation of quantum photon state manipulation. Several important applications are discussed, including computing and enhanced measurements. The review is clearly written, contains comprehensive list of references, and it will be certainly appreciated as a valuable contribution by the research community.

 I have the following comments and suggestions:

1. The review is fully focused on quantum effects, yet this is not reflected in the title. Consider changing the title to include word “quantum”.

We have added the word “quantum” to our title, thus changing to “The resurgence of the linear optics quantum interferometer—recent advances & applications”.

1. While the review is focused on general concepts, it would be useful to instructive a short summary of practical experimental achievements and limitations. For example, what size of unitary circuit was demonstrated? What are the losses in practical devices, what is the minimum loss and best fabrication fidelity achieved in basic optical elements like a coupler? Then, do such imperfections present fundamental barriers on scaling of circuit complexity?

While we agree that practical experimental achievements and limitations would be instructive, we have decided to focus on concepts in this review as it is what we do best. For the readers who would be interested in the experimental aspects of photonic quantum information processing, we have added a reference to a recent review by some Italian experimentalists. This can be found at top of page 2, in the following sentence “Experimental advancements and limitations of photonic implementations of quantum information processing are discussed at length in another review [12].”

3) In Fig. 1, it would be useful to show a current image as 1(a), and add in 1(b) a practical on-chip realization (i.e. use cropped Fig. 1 from <http://dx.doi.org/10.1126/science.aab3642>). This will give the readers a visual illustration on the state-of-the art of photonic chip manufacturing.

We have adapted and included Fig. 1 from Carolan *et al.* (Ref. [51]) as a current image of a Reck *et al*. type of decomposition, and its realization on an integrated photonic chip in Fig. 2. Fig. 1 of our paper has been kept as is, because it was referenced in the text as the original Reck *et al.* implementation. The decomposition of Carolan et al. is different.

4) When discussing spontaneous parametric down-conversion (SPDC) on page 2, it will be also useful to mention SFWM, and add recent reviews on integrated nonlinear photon sources: <https://doi.org/10.1515/nanoph-2016-0022> and <http://dx.doi.org/10.1016/j.revip.2016.11.003>

We have added a mention of SFWM along with SPDC in the first paragraph of page 2.

5) Sec. 3.3 mentions “fast switching” and “ultrafast measurement technique for time bins”. In would be good to give characteristic physical estimates of what “fast” and “ultrafast” are in seconds, Hz? What is the current technological level here, is it sufficient or further advances are needed?

We have added in Sec. 3.3 that “fast” optical switching typically occur withinin picoseconds. A more detailed discussion is given in a new section, Sec. 10, on optical switching. There we describe the different types of optical switching that are possible, and the speeds at which they can be implemented. We also point out there the requisite speed required for universal optical quantum computing, and the challenges we face getting to that speed.

6) Add a discussion of tomography <http://dx.doi.org/10.1038/NPHOTON.2011.283> and more recent works on sparsity concepts, i.e. <http://dx.doi.org/10.1364/OPTICA.3.000226> and <http://dx.doi.org/10.1364/OL.41.004079>

Based on Referee 2’s suggestion, we have added a new section on quantum state and process tomography (Sec. 6). Sparsity is mentioned in this section, and the above citations have been added.

7) In Sec. 8, add characteristic efficiencies (i.e. xx%) of different types of detectors. Also for PNR, mention maximum achieved photon-number resolution, and also technical difficulties (i.e. much lower operating temperature for TES). Although there is no space for a detailed description in this review, yet providing several characteristic experimental numbers will be very helpful for the readers.

We have added typical characteristics for the different types of in Table 1, and descriptions of limitations and technical difficulties in operating some of these detectors.

8) Check cited arXiv papers and replace with journal references if available – i.e. [78] was published as <http://dx.doi.org/10.1038/srep19489>

We thank the referee for pointing out the updated reference. We have revised the aforementioned reference, and also checked for other updates, revising where necessary.

In summary, this paper is recommended for publication after authors consider the above comments.

**Other revisions:**

1. Additional references have been brought to our attention and added to our review.
   1. In Section 4, we have added Phys. Rev. A 97 (2018) 022328 (ref. [55]), which shows a novel technique for decomposing unitary matrices. Its properties relative to the iconic Reck et al. decomposition and the newer Clemens et al. decomposition have been added in a discussion starting at the end of p. 4.
   2. In Section 11.4, we have added Phys. Rev. A 97 (2018) 032329 (ref. [207]) which makes use of continuous variable multipartite entanglement to achieve Heisenberg scaling in sensing a small phase shift that is distributed across multiple modes, i.e. the root-mean-square estimation error scales inversely with the number of modes.
   3. In Section 11.5, we have added the following developments in the rate of transmission of a lossy channel with entanglement assistance: i) a tighter bound than that of the TGW bound, which is given by Pirandola et al. in Nature Communications 8 (2017) 15043, ii) non-asymptotic rates derived by Wilde, Tomamichel and Berta in IEEE Transactions on Information Theory 63 (3) (2017) pp. 1792-1817 that are applicable for finite uses of the quantum channel, and iii) generalization of the TGW bound that applies to arbitrary network topology in Nature Communications 7 (2016) 13523.