Response Letter for manuscript #APL19-AR-06644 18 Sept 2019

Dear Editor,

We thank the reviewers for their detailed comments. Please find our response to the respective reviewers, and also editorial comments.

Reply to Reviewer 1:

We appreciate Referee 1's remarks, and his/her recommendation for its publication. In response to the suggestions, We changed the manuscript as follows:

1. **"Add labels to the Y axes in Fig. 5."**
   We have added the Y axes labels "Re" and "Im" to indicate the real and imaginary values of the respective density matrices, respectively.
2. **“Please do not use "new" and "novel"; if the findings are not new or novel, they should not be submitted to APL...”**
   We removed the “successful” in the abstract, and at one more location in the main text; we do not use words new, novel successful etc for any novelty claims anywhere. The occurance of “new” happens in a description of a Monte-Carlo process, the word novel does not appear, and the word “successful” is used on page 3, left col, 1 para as an attribute of the attack (*“This indicates a successful attack.”*). We don’t know of an alternative attribute to indicate that an attack has worked out, as compared to being unsuccessful – this appears the common term in English in this context.
3. **"Caption of Fig. 3: a remark about why ΔT remains the same from Block 15 to 16 could be added."**
   We included an explanation in the caption.
4. **"Names of the various polarizations |H>, ..., |A>, ..., |R> on pg 3 (left column) could be added."**
   We added the names of the respective polarization states.
5. **"...in the penultimate paragraph in the Supplementary material: Recent work assumed → Recent work erroneously assumed."**
   We have changed the text to be more forthcoming about the wrong assumption made in [15].

Reply to Reviewer 2:

We first address reviewer 2's concerns about the manuscript, especially with regards to its novelty and generality:

1. **"In paragraph 5, page 1, the authors claim that "We briefly review the clock synchronization protocol considered [15]". I think that the protocol mentioned by the authors should be cited as [10]."**

In our work, we examined the conclusions made in [15], which considered the effect of a circulator-based asymmetric delay attack (CADA) on the clock synchronization proposed in [10]. In this way, we think that "the clock synchronization protocol considered in [15]" is a more accurate statement and have not changed this statement in our manuscript.

2. **"The attacking method in this paper has been proposed in [15], and the experiment system is similar to [10] except additional circulators. Comparing with the citations [10] and [15], this work is more like a demonstrated comment to claim that the security measure proposed in [10] is invalid according to the attacking method in [15]."**
   Although Reviewer 2 correctly states that the attacking method (CADA) in the paper "has been proposed in [15]", and that our work demonstrated that "the security measure proposed in [10] is invalid according to the attack method in [15]", we would like to elaborate how these facts do not diminish the novelty of our work - they arose naturally from our efforts in developing the ideas presented in [10] and [15].

   In [15], a theoretical analysis concluded that the security measure proposed in [10] was effective against CADA, due to a measurable change in the distributed entangled state. In the present work, we highlight an erroneous assumption in [15], and verify experimentally our theoretical predictions after correcting the error - concluding that the protocol in [10], is in fact, ineffective against CADA. In this way, our results serve as original contributions addressing the security in [10] since they cannot be reproduced from [10] and [15] - they stand contrary to the conclusions made in [15].

   A similar observation was made regarding the significance of our contribution by Reviewer 1: "In Ref. 15, it was wrongly assumed that this dynamical phase is, “zero, or is known and compensated for”. In the current work, they find that this dynamical phase is likewise non-local and, more relevantly, combines with the geometric phase to produce no measurable net change in the state. They support this claim via an experimental quantum state tomography on the SPDC output."

   To emphasize this contribution of the work, we conclude the manuscript with an additional paragraph: "Our result corrects the prediction in Ref. 15, and clarifies the effectiveness of directly replacing classical signals with entangled photons to protect the synchronization channel -- we demonstrate that propagation delays can be introduced without affecting the entanglement degree-of-freedom, rendering the proposed protection ineffective against asymmetric delay attacks."

3. "**Although a circulator is a conventional device using in optical systems, the attacking method and its objective are too detailed."**
   We feel that the most convincing way to challenge a security claim is through a demonstration of a specific attack, and an analysis why it was successful.

   The attack objective was chosen to address the incorrect results presented in [15], which concluded erroneously that an asymmetric delay created by using a pair circulators can be detected with a Bell inequality check. We believe that our attack objective has the appropriate scope, since we target the two main features of the protocol in [10], i.e. (i) a symmetric synchronization channel and (ii) that the channel can be secured with a Bell inequality check - these are also the same features

considered in [15].

Regarding the specificity of our attack method, which demonstrated an asymmetric delay attack using two circulators, we believe that demonstrating a particular realization of the attack does not diminish the generality of our work. Our theoretical analysis was not tied to the use of a circulator, nor to a specific combination of circulators, but generally applies to any device that utilizes the time-reversal asymmetric property of Faraday-Rotation (FR) for creating an asymmetric delay in the synchronization channel.
Any FR-based attack that hopes to evade detection by the Bell inequality check proposed in [10] has to evolve the polarization state in a closed-cycle, which is the situation examined in our work. To experimentally realize a channel asymmetry using FR, we had to choose one specific device and deploy it in a manner that creates an asymmetric delay. Given the generality of our theoretical treatment, this choice does not diminish the generality of our work. Furthermore, to demonstrate the inefficacy of the Bell inequality check as a security layer against an asymmetric delay attack, it suffices to succeed only with one specific attack.

Finally, our work highlights the need to carefully examine the entanglement degrees-of-freedom (DOF) when developing a new protocol. In the synchronization protocol examined in this work and in [15], timing information is not encoded in the entanglement DOF. Moreover, a delay attack on the synchronization protocol using circulators, as demonstrated in our work, does not require an irreversible projection on the entanglement DOF. These two features distinguish the synchronization protocol from protocols that manage to achieve security through the use of entanglement (e.g. in the Ekert91 quantum key distribution protocol, information is directly encoded in the entanglement DOF), and serves as a valuable case study for the development of future entanglement-based protocols.

Reply to Editorial comments:

We received two rounds of editorial comments with overlaps; here the reply to the latest set received on 13 Sept 2019:

1. **“Figure 4 - Your tables and/or figures include a reference to a published work...”**
   Figure 4 has not been published elsewhere, the reference in the figure caption is just to acknowledge the origilal work of generating polarization-entangled photon pairs. The figure is not part of this or any other publication, hence no requirement of obtaining a permission to use. We also removed the reference from the figure cation, as this may have caused an automatic checking system to complain.
2. **“Please add the zip code to address 3 in the byline”.**
   We added the street address, including the ZIP code of address 3.
3. **“Please add figure sub-labels to Figure 5 (a) and (b).”**
   Sub-labels (a) and (b) were contained in the figure caption of the manuscript file, not in the figures themselves as there is also text for the respective fidelities with the Psi-state. However, we moved the sub-labels now above the image file to be consistent with other figures. We also combined the partial figures into a single one to perhaps prevent the automatic check system to complain again.
4. **“Please add a footnote naming and providing the email address for the corresponding author(s)”**

Added email address to the manuscript; however, it shows up as a), not as an asterisk, as in the current overleaf template on the APL website

List of changes:

1. **Abstract:** changed *"while successfully evading detection"* to *"while evading detection".*
2. **Authors:** Added corresponding author email address and fixed the street address of address line 3
3. **Pg 2 (right column):** changed "We use this result and experimentally demonstrate a successful asymmetric delay attack using the circulators in subsequent sections." to *"In subsequent sections, we use this result to experimentally demonstrate an asymmetric delay attack which evades detection."*.
4. **Pg 3 (left column):** changed *"... projects the polarization mode into either |H>,|V>,|D>,|A>,|L> or |R>."* to *"... projects the polarization mode into either horizontal, vertical, diagonal (+45 degrees), anti-diagonal (−45 degrees), left-circular, or right-circular polarization (|H>,|V>,|D>,|A>,|L> or |R>)."*.
5. **Pg 3, Fig. 3 (caption):** added *"The delay was created by redistributing the additional delays in Blocks 7 to 15, so that ΔT remains the same."*.
6. **Pg 3, Fig. 4 (caption):** we removed the reference to ref. 22 as the figure is not taken from there, but was only referencing to polarization entanglement via type-II SPDC. We left the reference in the appropriate section in the main text.
7. **Pg 4, Fig. 5a:** Y axis labels *"Re(\rho_o)"* and *"Im(\rho_o)"* were added.
8. **Pg 4, Fig. 5b:** Y axis labels *"Re(\rho)"* and *"Im(\rho)"* were added.
9. **Pg 4, Fig 5:** All subfigures were combined into a single file
10. **Pg 4, Figure 5:** we changed the text “before” and “after” to “with” and “without circulators”, both in the figure labels as well as in the caption text.
11. **Pg 4 (left column):** changed *"We have successfully demonstrated..."* to *"We have demonstrated..."*.
12. **Pg 4 (right column):** added *"Our result corrects the prediction in Ref. 15, and clarifies the effectiveness of directly replacing classical signals with entangled photons to protect the synchronization channel -- we demonstrate that propagation delays can be introduced without affecting the entanglement degree-of-freedom, rendering the proposed protection ineffective against asymmetric delay attacks."*
13. **Pg 4 (right column):** added section heading labeled "Supplementary Material".
14. **Pg 4 (right column):** changed *"In the supplementary material, we also ..."* to *"In the supplementary material, we ..."*.
15. **Pg 4 (right column)**: changed *"..., previously thought to be observable, as an additional phase ..."* to *"..., previously thought to be observable. We show that an additional phase ..."*.

16. **Pg 4 (right column):** moved *"We note that when geometric phases ... remains an open question."* to Supplementary material pg 2 (right column), last paragraph.
17. **Supplementary material pg 2 (right column):** *"Recent work assumed"* changed to *"Recent work wrongly assumed"*.
18. **Supplementary material pg 2 (right column)**: changed *"However, we note that the dynamic phase (Eq. S9)... "* to "*However, Eq. S9 shows that the dynamic phase ..."*.
19. **References:** updated Ref 11 from "arXiv preprint arXiv:1812.10077 (2018)" to "Phys. Rev. A 100, 023849 (2019)."
20. **References:** removed Ref 22 *"See supplementary material for a detailed evaluation of the geometric and dynamic phases imposed by the circulators."* because now there is an explicit statement at the end.

With this, we hope to have addressed the concerns with our manuscript, and look forward for your reply.

With Best Regards on behalf of all authors,

Christian Kurtsiefer