Secure Quantum Clock Synchronization

Antia Lamas-Linares[a] and James Troupe[b]

[a]Texas Advanced Computing Center, The University of Texas at Austin, Austin, Texas
[b]Applied Research Laboratories, The University of Texas at Austin, Austin, Texas

ABSTRACT

The ability to synchronize remote clocks plays an increasingly important role in our infrastructure, from maintaining coherence in the electrical grid to allowing precise positioning and navigation for civilian and military applications. However, many of the techniques to establish and maintain this time synchronization have been shown to be susceptible to interference by malicious parties. Here we propose a protocol that builds on techniques from quantum communication to provide a verified and secure time synchronization protocol. In contrast with classical protocols aimed at increasing the security of time distribution, we need not make any assumptions about the distance or propagation times between the clocks. In order to compromise the security of the protocol, an adversary must be able to perform quantum non-demolition measurements of the presence of a singe photon with high probability. The requirement of such quantum measurements raises a serious technological barrier for any would-be adversary.

Keywords: Clock Synchronization, Security, Quantum Communication, Quantum Optics, Metrology

1. INTRODUCTION

Keeping an accurate track of time and our ability to have remote clocks agree on the current time has been a subject of dedicated research efforts since at least 1714 when the British government established the Board of Longitude to find a method of reliably determining the longitude of ships at sea.[1]

As the culmination of this research, there now exist several Global Navigation Satellite Systems (GNSS): the first such system, the United States Global Positioning System (GPS), the European Union Galileo system, the Russian GLONASS, and China's soon to be completed BeiDou 3 system. While the common perception of the purpose of these networks is to provide precise and almost universally available positioning information, in reality these networks provide and distribute a more fundamental and even more widely useful resource: a precise and universal *common time reference*. The ubiquity of GPS and other GNSS timing signals has led to their utilization in many aspects of modern civilian society, e.g. computer networking, mobile phone networks, financial transactions networks, and electric power distribution. In addition, are a growing number of military applications that require a precision common time reference, such as distributed sensing, data fusion, secure communications, and electronic warfare.

However, given the critical and widespread reliance on distributed precision time, the security of these networks is generally quite weak. The signals that transfer time information can be spoofed by an adversary who wishes to disrupt or corrupt the timing networks.[2–4] While military use of GNSS does utilize additional security measures to detect and deter spoofing, these countermeasures generally add significant complexity and are still potentially vulnerable to sophisticated adversaries. Thus, there is a compelling need for fundamentally new methods for efficiently and securely distributing high precision time information. Due to the fact that even highly precise atomic clocks will drift relative to each other surprisingly quickly, a central requirement for the functioning of a secure time network is the ability to (re-)synchronize two clocks in a trusted manner.

In this paper we propose a protocol for secure time synchronization which is able to determine an absolute time offset between two remote clocks and does not rely on pre-existing knowledge of the relative position of the clocks or the propagation time of the signal used for synchronization. Using techniques from quantum

Further author information: (Send correspondence to Antia Lamas-Linares)
Antia Lamas-Linares: E-mail: alamas@tacc.utexas.edu, Telephone: 1 512 475 9266

communication, the proposed method is resistant against a broad class of spoofing attacks by a malicious party, an area of increasing interest in classical time distribution.

Quantum mechanical effects are at the heart of the best clocks in existence[5] but we will use the terms "quantum time synchronization protocols" in a more limited sense to refer to those protocols that use techniques related to quantum information for improving aspects of clock synchronization. There are several ways in which these quantum effects are utilized; some of the protocols focus on engineering the quantum state such that there is an improvement in the signal to noise ratio of the resulting measurement,[6,7] others share a large amount of prior entanglement and thus avoid both Einstein-style synchronization signals[8] and Eddington's slow clock transport,[9–11] another class exploits quantum effects to achieve immunity towards some environmental disturbances such as dispersion,[7,12] and yet another group uses measurements of the second order correlation function of photon pairs produced in SPDC.[13–16] It is this last technique, augmented with a symmetrization of the production and detection of the photon pairs, plus a security layer based on Bell inequalities, that constitutes the basis of our protocol for quantum secure clock synchronization.

Broadly speaking, clock synchronization refers to two different but related tasks.[5] The first is frequency distribution, where we are concerned with the difference in "ticking rates" between two separate clocks (syntonization). The second is that of time distribution where our concern is the offset at a particular instant between the reported time of two remote clocks. Most of this paper will focus on the later task. The discussion is organized as follows. In section 2 we will discuss the problem and how it is currently addressed using classical protocols and current technology. Section 3 will describe the quantum protocol and a proposed experimental layout.

Section 4 will address the security of the protocol against directionally asymmetric delays of the signals.

2. CLASSICAL CLOCK SYNCHRONIZATION

In this section we will review the requirements for securely establishing the offset between to distant clocks when using signals that convey only classical information. These requirements were recently clarified and reported by Narula and Humphreys[17] and we will closely follow their results here.

The problem: Alice and Bob are separated by some fixed distance and each possesses a local clock with an unknown difference in the times displayed by them. Choosing Alice's clock as the "Master" clock, we will refer to the difference time readings as the clock offset δ of Bob's clock. Thus, $t' = t + \delta$, where t is Alice's clock reading for an event and t' is Bob's clock reading for the same event assuming that Alice and Bob are co-located. When Alice and Bob are not co-located, a secure clock synchronization protocol attempts to measure and distribute information about the relative clock offset such that an adversary with access to the information channels used is unable to alter the inferred offset without being detected by Alice and Bob. Therefore, secure clock synchronization is an example of what we will call *secure metrology*, an interesting combination of the more common secure communication and metrology tasks.

2.1 One-Way Protocols

One-way classical clock synchronization protocols are based on the simple idea of Alice transmitting a signal (possibly using cryptographic authentication) containing a timestamp of the transmission time t according to her clock. Bob receives the signal and records the time of reception, t', according to his clock. If Bob knows the true propagation time between Alice and himself, Δt_{AB}, then he can calculate the offset via $\delta = t' - t - \Delta t_{AB}$. While this has the benefit of being a very simple protocol, it is inherently insecure since it assumes that the propagation time is known and not under the control of an adversary. Therefore, even if the signals used are authenticated and encrypted, one-way protocols are easily compromised by the introduction of a simple delay by an adversary, who we will call Damon, between Alice and Bob.

2.2 Two-Way Protocols

The main difference between the one-way and two-way protocols is the ability of Alice to estimate the propagation time between herself and Bob by measuring the round trip time (RTT). Under the assumption that the signal propagation time is directionally symmetric, the propagation time is half of the RTT. If the channel between Alice and Bob is known and accurately modeled, then Alice can compare the measured RTT to the RTT predicted by the model allowing her to detect any delay attacks that respect the assumed directional symmetry. As with all classical protocols, security also requires cryptographic authentication of the signals used to transmit the time information.

2.3 Requirements for Security of Classical Protocols

It is important to clarify what we mean by security in the context of clock synchronization. Unlike with cryptographic protocols, we do not yet have a formal mathematical definition of security. In clock synchronization, the basis for security is an essentially physical consideration of the abilities of an adversary within the laws of physics combined with whatever technical constraints are known (or assumed) to limit the adversary.

The following is one list of security requirements for all clock synchronization protocols that use classical signals:[17]

(1) Alice and Bob must use an authenticated encryption scheme to secure the signals used for transmitting timing information in order to prevent successful counterfeiting by Damon.

(2) The actual propagation time between Alice and Bob must not be reducible by more than a known, fixed amount L that will also set the accuracy limit of the synchronization protocol.

(3) The actual round trip time must be known *a priori* to Alice and must be measurable by Alice with an inaccuracy smaller than L.

The purpose of these requirements is to allow Alice the ability to use her clock to estimate the propagation time between her and Bob via the RTT of the photons. By comparing her estimates to the expected propagation time, Alice is able to detect Damon whenever the difference exceeds the limit L.

We close our discussion of the security of classical protocols by pointing out the significant limitations in the utility of the requirements above. The necessity of Alice (or Bob) knowing with significant precision what the true channel propagation time is *and* being able to place a trustworthy lower limit on the reducibility of this time are quite hard to satisfy. For example, in the simple case of free space propagation, it would require Alice and Bob to *a priori* have a trustworthy estimate of the relative distance between them. Furthermore, the precision of this distance estimate would set the secure limit for the precision of the clock synchronization protocol.

3. QUANTUM PROTOCOL

Entangled photon pairs produced by SPDC are extensively used in quantum information protocols. It has long been known[18] that the emission times of the photons in the pair are very tightly time correlated even if the emission event itself happens at random times. This can be exploited in clock synchronization protocols by measuring the second order correlation function.[13,14,16] The technique has also used extensively in non-pulsed quantum cryptography to find the relative time difference between Alice's and Bob's clocks and thus identify "coincidences" that correspond to the detection of two photons from the same pair. In such a scenario Alice and Bob each receive one member of a pair of photons produced with SPDC. They record the time of arrival with respect to their local clock and then calculate a cross-correlation of the times of arrival to extract the relative time of arrival difference as measured by their local clocks. Our protocol builds on this basic idea to detect coincident events, and augments it by situating a source of entangled photons both at Alice's and at Bob's lab and having each of them detect one member of the pair locally and send the other member of the pair to be detected at the other site, all while using a common propagation channel between their labs as illustrated in Fig. 1.

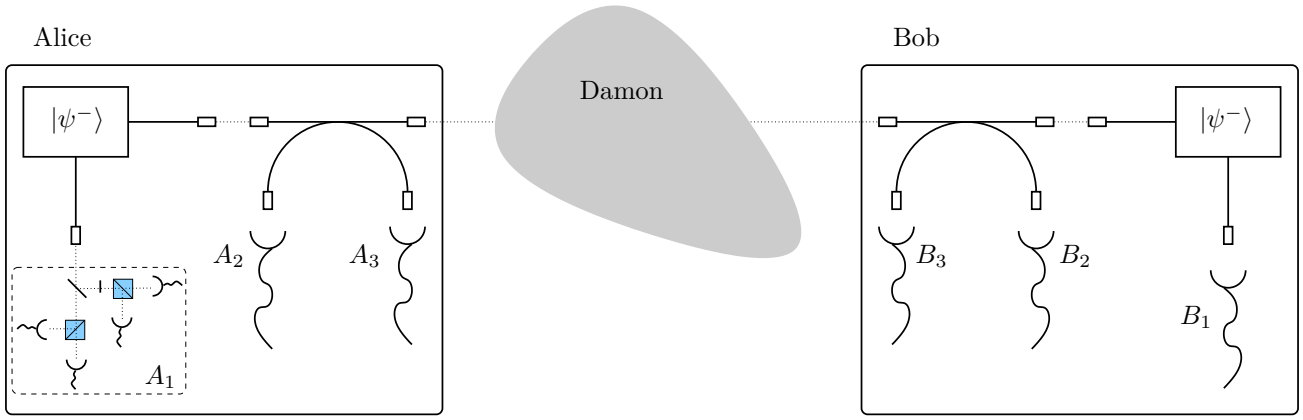

Figure 1. Proposed time synchronization experimental setup. Alice and Bob each have a source of polarization entangled pairs ($|\psi^-\rangle$) produced by spontaneous parametric down-conversion (SPDC) and a set of single photon detectors within their secure lab (denoted by a solid line). Each mode of propagation of the photons ends in a detector cluster able to perform polarization measurements, but only the cluster labeled as A_1 is fully represented in the figure. One member of the SPDC pair is detected locally at detector cluster A_1 in Alice's side and at cluster B_1 on Bob's side. The other member of the pair is sent into a single mode fiber and propagated through a channel controlled by an adversary, Damon. Each of the propagating photons has a chance of being detected on the remote side by A_2 or B_2 for pairs originating at Bob's and Alice's side respectively. Times of arrival for all detected photons are recorded in each lab with respect to a local clock. Detectors A_3 and B_3 are under the control of either Alice or Bob and are included for completion but do not play a part in the discussion. The detector cluster illustrated for A_1 represents a possible passive measurement scheme for a CSHS inequality. It uses a beam splitter followed by two polarizing beam splitters oriented at the appropriate angles for projection into the desired polarization state.

3.1 Time offset extraction

Following Ho et al.[15] we denote the numbers measured by Alice's (Bob's) local clock by t (t') with a subscript denoting a particular indexed event. If Alice and Bob were at the same spatial location detecting the same pair event, the difference between the times of detection as measured by their local clocks would be $\delta = t - t'$, and this δ would be the time offset that we aim to determine. If Alice and Bob are at separate locations, the time of propagation of a signal between Alice and Bob is denoted as Δt_{AB} (Δt_{BA} for propagation in the opposite direction). The round trip time of a signal originating from either Alice or Bob is $\Delta T = \Delta t_{AB} + \Delta t_{BA}$.

Additionally, since the channel is a single spatial mode and the signals propagating between Alice and Bob are identical in all degrees of freedom apart from propagation direction, we assume $\Delta t_{AB} = \Delta t_{BA} = \Delta t$. To calculate the absolute time difference between clocks, δ, consider a photon pair produced at Alice's site. One of the members of the pair is detected locally at detector A_1 and the other member of the pair travels to Bob accumulating a travel time Δt_{AB} and getting detected at B_2. For any particular pair event produced at Alice's site, the difference between the time labels recorded at Alice and Bob will be:

$$t' - t = \Delta t_{AB} + \delta.$$

Similarly for any pair produced at Bob's site:

$$t - t' = \Delta t_{BA} - \delta.$$

These differences between the time labels can be extracted by calculating a cross-correlation between events at both sides. Consider first events produced on Alice's site. The detection events are translated into a function as:

$$\begin{aligned} a(t) &= \sum_i \delta\left(t - t_i\right) \mathrm{d}t \\ b(t') &= \sum_j \delta\left(t - t'_j\right) \mathrm{d}t. \end{aligned}$$

Where i and j just index arbitrary detection events which can arise either from pairs or from other detector triggers such as stray light, dark counts, etc. The cross-correlation is computed as:

$$c_{AB}(\tau) = (a \star b)(\tau) = \int a(t)b(t+\tau)\mathrm{d}t,$$

and will have a maximum at $\tau = \tau_{AB} = \Delta t_{AB} + \delta$. Likewise if we consider those pairs created on Bob's site, we can extract another cross-correlation,

$$c_{BA}(\tau) = (b \star a)(\tau) = \int b(t)a(t+\tau)\mathrm{d}t,$$

which will have a maximum at $\tau = \tau_{BA} = \Delta t_{BA} - \delta$.

From these we can extract both the round trip time and the absolute time difference between clocks without making any prior assumptions about the length of the path between Alice and Bob.

$$\begin{aligned} \Delta T &= \tau_{AB} + \tau_{BA} \\ \delta &= \frac{1}{2}\left(\tau_{AB} - \tau_{BA}\right). \end{aligned}$$

3.2 Security

The time extraction protocol we just described includes several assumptions which need to be carefully examined if we are performing this protocol in an adversarial context. The first assumption we are making is that the signals that each party is receiving are truly originating as part of the same pair. Fortunately the entanglement of the pairs provides us a built in mechanism to ascertain exactly this. A measurement of a Bell inequality in the polarization degree of freedom will ensure that the pairs we are measuring and correlating to each other do indeed belong together. This check also ensures that the polarization degree of freedom has not been accessed by our adversary to extract any information as this would affect the results of the Bell inequality.

A Bell inequality in the polarization degree of freedom does not by itself guarantee that the timing information has not been manipulated. For example, an adversary could introduce an arbitrary delay that is polarization insensitive and this would not be detected in any meaningful way, as the effect would be to change the calculated values of τ_{AB} and τ_{BA}. In a nutshell this is why conventional one way protocols are vulnerable to delay attacks, and even classical two way protocols need to impose strong conditions for security. For the protocol proposed here, a time delay introduced in this manner would have no effect on the calculated clock time offset δ because of the symmetrization of the sources and detection.

We are thus left with one final assumption, that of symmetry of the propagation times through the channel (i.e. $t_{AB} = t_{BA}$). This case can be formalized as the adversary, Damon, introducing an arbitrary delay added to the un-modified values,

$$\begin{aligned} \Delta t^d_{AB} &= \Delta t + D_1 \\ \Delta t^d_{BA} &= \Delta t + D_2. \end{aligned}$$

If $D_1 \neq D_2$ and Alice and Bob believe the channel to be symmetric, then they would arrive at a Damon-determined value of δ^d:

$$\begin{aligned} \tau^d_{AB} &= \Delta t^d_{AB} + \delta^d \\ \tau^d_{BA} &= \Delta t^d_{BA} - \delta^d \\ \delta^d &= \frac{1}{2}\left(\tau^d_{AB} - \tau^d_{BA}\right) = \delta + \frac{1}{2}\left(D_1 - D_2\right). \end{aligned}$$

Thus, the time difference estimated by Alice and Bob would be off from the true value by one half of the magnitude of the unknown asymmetry.

It is worth now carefully revisiting the possible interference by an adversary. A first mode of attack has Damon modifying our measured values times of arrival of the photon pairs. For the source based at Alice's site, he clearly cannot influence the member of the pair that is detected locally, as this is all within Alice's secure area. He could modify Bob's detected time of arrival of the signals coming from Alice in a consistent way, but this would be equivalent to introducing a –possibly asymmetric – delay on the channel. Thus, we are left with the question of under what circumstances Damon can introduce an a delay that is different depending on the direction in which the signal is propagating (or depending on whether the photon originates at Alice or at Bob).

3.3 Step by step protocol description

1. Alice and Bob each have a source of polarization entangled photons within their secure laboratories.

2. One photon from each pair produced is detected locally and labeled according to a local clock. For Alice the local detection happens in detector group A_1 and is tagged with times $t_1, t_2, \ldots, t_i$. The other photon produced at Alice's site is sent through the channel to Bob's laboratory, detected at B_2 and is tagged with times $t'_1, t'_2, \ldots, t'_j$. Likewise for photon pairs produced at Bob's site we would have detections at B_1 and A_2 with time tags $t'_1, t'_2, \ldots, t'_k$ and $t_1, t_2, \ldots, t_m$ respectively.

3. Time offset extraction: Alice and Bob exchange over a public authenticated channel the time tags of photon detection times as measured by their local clocks and calculate a cross-correlation between detector cluster times A_1 and B_2, and between B_1 and A_2. With this they are able to extract the time offset δ and round trip time ΔT using the procedure described previously.

4. Security check: With the timing offset determined, Alice and Bob check the correlations between the individual detectors in groups A_1 and B_2 and groups B_1 and A_2. The violation of a CHSH inequality verifies the origin of the pairs.

5. Additionally, Alice and Bob need to randomly sample the population of photons to check that photons from Alice and from Bob are truly indistinguishable, as any distinguishability would provide a vector for Damon to introduce an asymmetric delay.

3.4 Performance and implementation

The implementation of this protocols uses the same basic toolkit as an entanglement-based QKD experiment.[19] The main components are: polarization entanglement sources, single mode fibers, an optical channel, an authenticated classical channel, single photon detectors and time tagging hardware. The cross-correlation can be performed with very limited computational hardware by carefully tailoring the FFT calculation[15] with only a few seconds of noisy data and not particularly good local clocks, as has been demonstrated in free-space QKD experiments.

The timing performance is fundamentally limited by a combination of detector jitter, channel jitter and intrinsic width of the second order correlation function of the PDC emission. In our protocol we additionally have possible interference by a malicious party and deviations from an ideal violation of a Bell inequality can affect the confidence on our time offset measurements. A recent experiment by Quan et al.[16] that uses PDC for synchronization has demonstrated an absolute time accuracy of just under 60 ps, limited by detector and time tagging hardware, and shown that values below 10 fs are in principle possible. A full analysis of the expected performance is currently in preparation.

4. SECURITY AGAINST DELAY ATTACKS

The security of the quantum protocol is derived from a few fundamental properties of the entangled photons used to measure the clock offset: (1) the photons are emitted from Alice's and Bob's positions at fundamentally random times, (2) both Alice's and Bob's photons travel (in opposite directions) in the same single spatial mode, (3) the sources are designed to have the same spectra, and (4) the polarization states of the transmitted photons can't be copied with high fidelity by an adversary without detection. Notice that given the above, the direction of travel of a given photon is completely uncorrelated with any of its other degrees of freedom. This implies there

is no possible way for Damon to simply filter the photons using one of the other degrees of freedom in order to isolate a photon's direction of travel and break reciprocity of the channel.

In order for an adversary to compromise the security of the quantum protocol, he must alter the propagation of photons in the single spatial mode between Alice and Bob such that a photon traveling in one direction experiences a different propagation time than one traveling in the opposite one. Therefore, Damon must find some way to measure the direction of travel of the photons in the channel such that (1) he knows (or at least has a high probability of knowing) *when* the direction measurement is successful, and (2) when successful, the direction measurement is *non-destructive* – both in the sense of not destroying the photon (e.g. by it being absorbed) and not altering any other degree of freedom of the photon. The first requirement comes from the fact that for success, Damon must know *when* a photon is passing him by in a particular direction in order to apply his chosen propagation delay, and when unsuccessful, he needs to filter out the photons he was unable to alter.

We note that if Damon has the ability to perform a Quantum Non-Demolition (QND) measurement of the presence of a photon with high success probability at two points along the channel, then he would be able to satisfy both of the requirements above and therefore could break the security of the quantum protocol. However, the technical requirements for accomplishing such QND measurements[20–22] or directly creating a controllable coherent single photon nonreciprocity[23–25] in th channel are currently a serious impediment to implementing this strategy. Also, notice that the first condition for breaking the protocol implies that at least one such QND measurement is always needed for Damon's success. This is true since Demon must know with high probability *when* a photon is present in the channel at a particular location (and direction) in order to impose different path delays. We therefore conclude that the proposed quantum clock synchronization protocol is secure when the adversary does not have the capability to perform a QND measurement of the presence of a single photon.

5. CONCLUSIONS

In this article we introduce a new method of synchronizing two distant clocks that utilizes the properties of polarization entangled photon pairs from a spontaneous parametric down-conversion source to simultaneously distribute precise relative time information and provide the ability to authenticate this information. Authentication is achieved by verification of quantum entanglement between the two parties by observing violation of a CHSH inequality. Furthermore, the inferred relative clock offset is secure against passive delay attacks due to the symmetry of the protocol, and is secure against active delay attacks on individual photons because of the significant technological difficulty of producing non-destructive and non-disturbing interactions that can break the reciprocity of the single mode channel between Alice and Bob at the single photon level and with high success probability.

In addition to improved security over classical clock synchronization methods, this quantum protocol also does not require upper and lower bounds on propagation times between the two parties be known *a priori*. This removes any need for precise and trustworthy modeling of the communication channel or knowledge of the relative positions of the two parties, opening the possibility of ad-hoc clock synchronization between mobile stations.

In future work we will develop the proposed secure clock synchronization protocol further by analyzing the precision of the clock offset estimate as a function of the characteristics of the PDC sources, optical channel, and detectors. We will also analyze how the *secure* precision of the protocol, i.e. the achievable precision of the clock offset that is trustworthy, changes as a function of the channel noise as well as source and detector non-idealities.

ACKNOWLEDGMENTS

The authors would like to thank the Centre for Quantum Technologies in Singapore for graciously hosting them for an extended visit during which some of this work was completed. The authors also thank Christian Kurtsiefer and Alessandro Cere for useful discussions. AL-L acknowledges support from the Texas Advanced Computing Center. JT acknowledges support from the ARL:UT Independent Research and Development Program.

REFERENCES

[1] Sobel, D., [*Longitude: The True Story of a Lone Genius Who Solved the Greatest Scientific Problem of His Time*], Walker Publishing Company (1995).

[2] Shepard, D. P., Humphreys, T. E., and Fansler, A., "Evaluation of the vulnerability of phasor measurement units to GPS spoofing attacks," *International Journal of Critical Infrastructure Protection* **5**, 146 (2012).

[3] Kerns, A. J., Shepard, D. P., Bhatti, J. A., and Humphreys, T. E., "Unmanned aircraft capture and control via GPS spoofing," *Journal of Field Robotics* **31**, 617 (2014).

[4] Bhatti, J. and Humphreys, T. E., "Hostile control of ships via false GPS signals: Demonstration and detection," *NAVIGATION: Journal of the Institute of Navigation* **64**(1), 51 (2017).

[5] Levine, J., "Introduction to time and frequency metrology," *Review of Scientific Instruments* **70**, 2567 (1999).

[6] Chuang, I. L., "Quantum algorithm for distributed clock synchronization," *Physical Review Letters* **85**, 2006 (2000).

[7] Giovannetti, V., Lloyd, S., and Maccone, L., "Quantum-enhanced positioning and clock synchronization," *Nature* **412**, 417 (2001).

[8] Einstein, A., "Zur electrodynamic bewegter körper," *Annalen der Physik* **17**, 891 (1905).

[9] Eddington, A. S., [*The Mathematical Theory of Relativity*], Cambridge University Press (1924).

[10] Jozsa, R., Abrams, D. S., Dowling, J. P., and Williams, C. P., "Quantum clock synchronization based on shared prior entanglement," *Physical Review Letters* **85**(9), 2010 (2000).

[11] Ilo-Okeke, E. O., Tessler, L., Dowling, J. P., and Byrnes, T., "Remote quantum clock synchronization without synchronized clocks," *Pre-print* , arXiv:1709.08423 (2017).

[12] Giovannetti, V., Lloyd, S., Maccone, L., Shapiro, J. H., and Wong, F. N. C., "Conveyor-belt clock synchronization," *Physical Review A* **70**, 043808 (2004).

[13] Bahder, T. B. and Golding, W. M., "Clock synchronization based on second-order quantum coherence of entangled photons," *AIP Conference Proceedings* **734**, 395 (2004).

[14] Valencia, A., Scarcelli, G., and Shih, Y., "Distant clock synchronization using entangled photon pairs," *Applied Physics Letters* **85**, 2655 (2004).

[15] Ho, C., Lamas-Linares, A., and Kurtsiefer, C., "Clock synchronization by remote detection of correlated photon pairs," *New Journal of Physics* **11**, 045007 (2009).

[16] Quan, R., Zhai, Y., Wang, M., Hou, F., Wang, S., Xiang, X., Liu, T., Zhang, S., and Dong, R., "Demonstration of quantum synchronization based on second-order quantum coherence of entangled photons," *Scientific Reports* **6**, 30453 (2016).

[17] Narula, L. and Humphreys, T., "Requirements for secure clock synchronization," *Pre-print* , arXiv:1710.05798 (2017).

[18] Hong, C. K., Ou, Z. Y., and Mandel, L., "Measurement of subpicosecond time intervals between two photons by interference," *Physical Review Letters* **59**, 2044 (1987).

[19] Ling, A., Peloso, M. P., Marcikic, I., Scarani, V., Lamas-Linares, A., and Kurtsiefer, C., "Experimental quantum key distribution based on a bell test," *Physical Review A* **78**, 020301 (R) (2008).

[20] Imoto, N., Haus, H. A., and Yamamoto, Y., "Quantum nondemolition measurement of the photon number via the optical kerr effect," *Physical Review A* **32**, 2287 (1985).

[21] Xiao, Y.-F., Şahin Kaya Özdemir, Gaddam, V., Dong, C.-H., Imoto, N., and Yang, L., "Quantum nondemolition measurement of photon number via optical kerr effect in an ultra-high-Q microtoroid cavity," *Optics Express* **16**, 21462 (2008).

[22] Reiserer, A., Ritter, S., and Rempe, G., "Non destructive detection of an optical photon," *Science* **342**, 1349 (2013).

[23] Hafezi, M. and Rabl, P., "Optomechanically induced non-reciprocity in microring resonators," *Optics Express* **20**, 7672 (2012).

[24] Lenferink, E. J., GuohuaWei, and Stern, N. P., "Coherent optical non-reciprocity in axisymmetric resonators," *Optics Express* **22**, 16099 (2014).

[25] Shen, Z., Zhang, Y.-L., Chen, Y., Zou, C.-L., Xiao, Y.-F., Zou, X.-B., Sun, F.-W., Guo, G.-C., and Dong, C.-H. *Nature Photonics* **10**, 657 (2016).