Asymmetric delay attack on an entanglement-based bidirectional clock synchronization protocol

Jianwei Lee,1 Lijiong Shen,1,2 Alessandro Cerè,1 James Troupe,3 Antia Lamas-Linares,4,1 and Christian Kurtsiefer1,2
1) Centre for Quantum Technologies, National University of Singapore, 3 Science Drive 2, Singapore 117543, Singapore
2) Department of Physics, National University of Singapore, 2 Science Drive 3, Singapore 117551, Singapore
3) Applied Research Laboratories, The University of Texas at Austin, Austin, Texas, USA
4) SpeQtral, 73 Science Park Drive, Singapore 118254, Singapore

(Dated: 21 February 2022)

We demonstrate an attack on a clock synchronization protocol that attempts to detect tampering of the synchronization channel using polarization-entangled photon pairs. The protocol relies on a symmetrical channel, where propagation delays do not depend on propagation direction, for correctly deducing the offset between clocks—a condition that could be manipulated with optical circulators, which rely on static magnetic fields to break the reciprocity of propagating electromagnetic fields. Despite the polarization transformation induced within a set of circulators, our attack creates an error in time synchronization while successfully evading detection.

I. INTRODUCTION

Clock synchronization protocols that bidirectionally exchange signals, e.g., the Network Time Protocol (NTP) or the two-way satellite time transfer (TWSTFT), are widely used to estimate the absolute time offset between remote clocks without first characterizing network propagation times. By assuming that propagation delays are symmetric in the two directions of travel in a synchronization channel, parties estimate one-way propagation times as half of the round-trip time. Although convenient, this assumption exposes the protocol to attacks that introduce unknown asymmetric channel delays which cannot be detected by better encryption or authentication. Existing countermeasures, e.g., based on monitoring round-trip times have been evaded by sophisticated intercept, spoofing and delay techniques.

Recently, protocol implementations using entangled photons suggest measuring non-local properties to ensure that synchronization networks have not been tampered with—a technique associated with entanglement-sure that synchronization networks have not been tampered with—an attack that could be manipulated with optical circulators, which rely on static magnetic fields to break the reciprocity of propagating electromagnetic fields. Despite the polarization transformation induced within a set of circulators, our attack creates an error in time synchronization while successfully evading detection.

II. ATTACKING AN ENTANGLEMENT-BASED CLOCK SYNCHRONIZATION PROTOCOL

We briefly review the clock synchronization protocol considered. The protocol involves two parties, Alice and Bob, connected by a single mode optical channel. Each party has a source of polarization-entangled photon pairs generated by SPDC. One photon of the pair is detected locally, while the other is sent and detected on the remote side (Figure 1). Every photodetection event is time-tagged with respect to a local clock which assigns time stamps to and t'.

Photon pairs emerging from SPDC are tightly time-correlated. Thus, for an offset δ between the clocks, a propagation time \( \Delta t_{AB} \) from Alice to Bob, and \( \Delta t_{BA} \) in the other direction, the second-order correlation function \( G^{(2)}(\tau = t' - t) \) of the time difference has two peaks at

\[ \tau_{AB} = \delta + \Delta t_{AB} \quad \text{and} \quad \tau_{BA} = \delta - \Delta t_{BA} \]  

(1)

due to pairs created by Alice and Bob. A round-trip time \( \Delta T \) for photons can be calculated using the inter-
peak separation,
\[ \Delta T = \Delta t_{AB} + \Delta t_{BA} = \tau_{AB} - \tau_{BA}. \]  
(2)

while the offset
\[ \delta = \frac{1}{2} \left[ (\tau_{AB} + \tau_{BA}) - (\Delta t_{AB} - \Delta t_{BA}) \right] \]
(3)

is given by the midpoint of the peaks and a propagation delay asymmetry, respectively. Assuming a symmetrical propagation delay, \( \Delta t_{AB} = \Delta t_{BA} \), the clock offset
\[ \delta = \frac{1}{2} (\tau_{AB} + \tau_{BA}) \]
(4)

is obtained directly from the midpoint.

Eve may now may exploit this assumption by separating the two propagation directions with a pair of circulators (Figure 1, gray region), introducing a direction-dependent delay \( \Delta t_{AB} - \Delta t_{BA} = (L - L')/v \), where \( L \) is the additional propagation length from Alice to Bob, and \( L' \) in the other direction, and \( v \) is the speed of light in the fiber. If Alice and Bob continue to rely on the midpoint between the peaks to estimate \( \delta \), they will obtain instead \( \delta + (L - L')/2v \).

In an attempt to detect the circulators, Ref. 15 suggests that Alice and Bob monitor polarization correlations using avalanche photodiode preceded by a polarization measurement in the appropriate bases (DA,B). The detection scheme is based on the fact that circulators use Faraday Rotation to separate photons propagating in opposite directions - Faraday Rotation is a time-reversal symmetry breaking mechanism that rotates polarization, potentially changing the input state.

For each individual polarization state to be preserved, the circulators must rotate the state by an integer multiple of 180° so that for a Bell state \( |\Psi^-\rangle = \frac{1}{\sqrt{2}}(|HV\rangle - |VH\rangle) \) distributed by Alice, the rotation of Bob’s state \( (|\psi_B\rangle \rightarrow \pm |\psi_B\rangle) \) does not result in any measurable change
\[ |\Psi^-\rangle \rightarrow \frac{1}{\sqrt{2}} (|HV\rangle - |VH\rangle) = \pm |\Psi^-\rangle. \]  
(5)

However, as the evolution of Bob’s state follows a closed trajectory on the Poincaré sphere, Ref. 15 predicted that a geometric phase – the phase determined by the geometry of the trajectory on the sphere(15) – is imposed on the Bell state, and can be detected in a non-local measurement. We show in the supplementary material that when other phase contributions are taken into account, the net effect of the circulators nonetheless produce no measurable change to the Bell state (Eq. 5). We use this result and experimentally demonstrate a successful asymmetric delay attack using the circulators in subsequent sections.

III. EXPERIMENT

We first implement the clock synchronization protocol. For two independent rubidium clocks, the following setup was previously characterized to achieve a synchronization precision of 51 ps in 100 s, comparable to the relative intrinsic frequency instability of each clock(10).

Two identical SPDC sources generate polarization-entangled photon pairs (Figure 1). The output of a laser diode (power \( \approx 10 \) mW, central wavelength 405 nm) is coupled into a single mode optical fiber (SMF) for spatial mode filtering and focused to a beam waist of 80 μm into a 2 mm thick β-Barium Borate crystal cut for non-collinear type-II phase matching(22). Down-converted photons at 810 nm are coupled into two single mode fibers with an overall detected pair rate of about 200 s\(^{-1}\). Fiber beam splitters separate the photon pairs so that one photon is detected locally with an avalanche photodetector (DA,B), while the other photon is transmitted to the remote party.

Time-stamping units assign detection times \( t \) and \( t' \) to the events detected at Alice and Bob, respectively. We compute the histogram \( G(2)(\tau = t' - t) \) of the time differences and resolve two coincidence peaks (FWHM \( \approx 500 \) ps) with a resolution of 16 ps, one from each source(23). The offset and round-trip-times are determined from the mean and separation of the peaks, respectively. For the purposes of this demonstration, we lock the clocks with unknown offset to a common rubidium frequency reference, thus avoiding frequency drifts that can detract from the main point of the experiment, i.e. demonstrating an induced error in offset estimation.

A. Asymmetric Delay Attack

To implement the asymmetric delay attack, we use two 3-port polarization-insensitive optical circulators of design-wavelength 810 nm and two single mode fibers of lengths \( L \) and \( L' \).

FIG. 1. Clock synchronization scheme. Alice and Bob each have a source of polarization-entangled photon pairs \( |\Psi^-\rangle \), and avalanche photodetectors at DA,B. One photon of the pair is detected locally, while the other photon is sent through a fiber to be detected on the remote side. Arrival times for all detected photons are recorded at each side with respect to local clocks, each locked to a rubidium frequency reference. Grey region: asymmetric delay attack. An adversary (Eve) uses a pair of circulators to introduce a direction-dependent propagation delay: photons originating at Bob’s site will always take the bottom path, while photons originating at Alice’s side will take the top path.
We first estimate the initial offset \(\delta_o\) between the two clocks with a symmetric channel delay \(L = L' = L_o\). Figure 2(a) shows \(g^{(2)}(\tau)\), the second-order correlation function \(G^{(2)}(\tau)\) normalized to background coincidences, acquired from the time stamps recorded for about 5 min. In Figure 3 we plot the offset and round-trip times estimated every 40 s.

To illustrate the difference in the cross-correlation measured between a symmetric and an asymmetric delay attack, we use two 5 m fibers to impose an additional round-trip of 10 m, but distribute them differently during each attack. For the symmetric delay attack, we extend \(L\) and \(L'\) equally by 5 m. We observe in Figure 2(b) that although the peak separation increases, the midpoint of the peaks used for estimating the offset remains unchanged. For the asymmetric delay attack, both fibers are used to extend \(L\) by 10 m, while \(L'\) remains unchanged. We observe in Figure 2(c) that the peak separation remains the same as in Figure 2(b), but the midpoint of the peaks has shifted by 25.24 (2) ns corresponding to half the additional round-trip time incurred. This indicates a successful attack.

### B. Asymmetric Delay Attack Detection

As a proof-of-principle demonstration of how the circulators influence the distributed entanglement, we measure polarization correlations of Alice’s pair source before and after the circulators are inserted in one of its output modes with the setup shown in Figure 4. For each output mode, a quarter-wave plate (QWP), half-wave plate (HWP) and polarizing beamsplitter (PBS) projects the polarization mode into either \(|H\rangle, |V\rangle, |D\rangle, |A\rangle, |L\rangle\) or \(|R\rangle\). Fiber polarization controllers (FPCs) correct for the polarization errors introduced by the fibers. We note that since FPCs do not break time-reversal symmetry, they cannot invert the polarization transformation induced by the circulators. We detect photon pairs with APDs for 36 wave plate settings and numerically search for the density matrix most likely to have returned the observed pair rates.

Figure 5 shows the reconstructed density matrices of Alice’s state before \((\rho_o)\) and after \((\rho)\) the introduction of the circulators into the path of Bob’s photons. We compare \(\rho_o\) and \(\rho\) by computing the fidelity \(F(\rho, \rho_o) = \langle \psi^- | \rho | \psi^- \rangle\).
FIG. 6. Fidelity distribution comparing the Bell state originating from Alice’s source before and after introducing the circulators. The density matrices obtained (a) before and (b) after polarization-insensitive circulators are inserted (Figure 4) do not deviate significantly from $|\Psi^\pm\rangle$.

(a) Before insertion of circulators, fidelity with $|\Psi^+\rangle$: 98.2%.

(b) After insertion of circulators, fidelity with $|\Psi^-\rangle$: 98.4%.

FIG. 6. Fidelity distribution comparing the Bell state originating from Alice’s source before and after introducing the circulators. The distribution is generated by numerically propagating errors due to counting statistics. A high mean fidelity suggests that the state remains unchanged and cannot be used to detect the attack. Error bars: Poissonian standard deviation.

$\left(\text{Tr}\sqrt{\rho_0}\sqrt{\rho}\right)^2$. The uncertainty in $F$ due to errors in counting statistics was obtained by Monte Carlo simulation, where 36 new measurement results are numerically generated, each drawn randomly from a Poissonian distribution with a mean equal to the original number of counts. From these numerically generated results, a new density matrix can be calculated and consequently, a new value of $F$. Repeating this process 100 times, we obtain the fidelity distribution shown in Figure 6, from which we compute a 95% confidence interval $98.7% < F < 98.9%$. The distribution of $F$ does not include 100%, which we attribute to imperfect control of the polarization state in the optical fiber. From the near-unity value of $F$, we conclude that the circulators do not affect the distributed Bell state.

IV. CONCLUSION

We have successfully demonstrated an attack of a clock synchronization protocol that tries to achieve security by detecting changes in polarization-entanglement distributed across a synchronization channel. The attack was implemented by rerouting photons with polarization-insensitive circulators, and imposing a direction-dependent propagation delay. The observed shift in the estimated clock offset is equal to half the propagation delay asymmetry, as expected for a protocol which assumes a symmetric channel. Although circulators reroute photons using a polarization-rotation mechanism, we experimentally verify that they produce no measurable change in the distributed entangled state, indicating that they cannot be detected with the protocol.

In this work, we focused on detecting its underlying mechanism – Faraday Rotation (FR), which must be performed in any circulator. Methods based on characterizing light intensities, e.g. identifying additional reflections, may still allow the detection of circulators, but they rely on the specific characteristics of the device (e.g. reflectivity). We also note that when Alice and Bob exchange photons that are identical in every other degree-of-freedom apart from propagation direction, there are few technologies besides a FR-based circulator capable of discreetly separating their photons. Alternatives such as advanced photonic structures and quantum non-demolition measurements still pose a significant technological barrier for any adversary, so entanglement-based clock synchronization still may provide a significant security advantage compared to traditional methods.

In the supplementary material, we also examine the geometric phase associated with polarization state rotation in the circulators, previously thought to be observable, as an additional phase associated with photon dynamics in the Faraday Rotator neutralizes this geometric phase. We note that when geometric phases were observed in other entangled systems, an interferometric arrangement was necessary to eliminate the influence of this “dynamic” phase. Whether or not a similar technique can be used to secure the present synchronization protocol remains an open question.

We acknowledge support by the National Research Foundation & Ministry of Education in Singapore. JT acknowledges support from the ARL:UT Independent Research and Development Program.
In this section, we show that when circulators rotate the polarization state of one of the photons in an entangled pair by 180°, the geometric phase imposed on the rotated photon does not produce a measurable change in polarization entanglement.

We first introduce the formalism to deal with the fact that points on the Poincaré sphere carry no phase information: the beginning and endpoints of a cyclic evolution correspond on the same point on the sphere.

To reflect this property, we define a “basis vector field” \( |\tilde{\psi}(t)\rangle\), such that

\[
|\tilde{\psi}(t)\rangle = e^{-i f(t)}|\psi(t)\rangle \quad \text{and} \quad |\tilde{\psi}(\tau)\rangle = |\tilde{\psi}(0)\rangle,
\]

where \( f(t) \) is the phase of \( |\psi(t)\rangle \) expressed in terms of its basis state \( |\tilde{\psi}(t)\rangle \) on the Poincaré sphere\(^{30}\).

The change in \( f \) comprises of two terms

\[\Delta f = \beta + \gamma,\]

where the geometric phase

\[
\beta = \int_0^\tau \langle \tilde{\psi}(t)|i\frac{d}{dt}|\psi(t)\rangle dt
\]

is due to the evolution of the basis state along a curved geometry, and the dynamic phase

\[
\gamma = -\int_0^\tau \langle \psi(t)|i\frac{d}{dt}|\psi(t)\rangle dt
\]

is due to the photon’s dynamics through the rotation medium\(^{19}\).

1. Geometric Phase

Berry showed that the geometric phase is proportional only to the solid angle \( \Omega \) subtended by the cyclic trajectory on the Poincaré sphere\(^{116}\):

\[\beta = -\frac{\gamma}{2} \Omega.\]  

Thus, a qubit in the initial state

\[
|\psi(t = 0)\rangle = e^{-i \phi \cos(\theta/2)}|R\rangle + \sin(\theta/2)|L\rangle
\]

that underwent a 180° rotation in the plane of polarization \( \phi \rightarrow \phi + 2\pi \) will accumulate a geometric phase \( \beta = -\pi(1 - \cos \theta) \).

2. Dynamic Phase

To evaluate the dynamic phase \( \gamma \) accumulated by the photon at end of a Faraday Rotator of length \( d \), we pa-
rameterize its expression in Eq. A3 in terms of the penetration depth $z$
\[\gamma = -\int_0^d \langle \psi(z)|i\frac{d}{dz}|\psi(z)\rangle dz = -\int_0^d \langle \psi(z)|\hat{N}|\psi(z)\rangle dz, \tag{A6}\]

where
\[\hat{N} = k \left( \begin{array}{cc} n_R & 0 \\ 0 & n_L \end{array} \right) \quad \text{and} \quad |\psi(z)\rangle = \left( e^{i kn_R z e^{-i\phi} \cos(\theta/2)} e^{i kn_L z \sin(\theta/2)} \right)\]

are expressed in the $\{ |R\rangle, |L\rangle \}$ basis, and $k = \frac{2\pi}{\lambda}$ is the wave number of the photon mode in free space.

The Faraday Rotator is a birefringent medium whose refractive indices $n_{R,L}$ depend on the magnitude of an applied magnetic field $B$ in the direction of light propagation,
\[n_{R,L} = n_0 \left( 1 \pm \frac{VB}{kn_0} \right), \tag{A8}\]

where $V$ is the Verdet constant and $n_0$ is the index of refraction in the absence of a magnetic field.

Substituting A7 into A6 we obtain
\[\gamma = kn_0 d + VBd \cos \theta, \tag{A9}\]

where the product $VBd$ can be shown to be the anti-clockwise rotation angle for a linearly polarized input.

Consider an initial input state $|\psi(\phi = 0, \theta = 0)\rangle = |H\rangle$. For the evolution cycle ($\phi = 0 \rightarrow 2\pi$) considered earlier, $|H\rangle \rightarrow |-45\rangle \rightarrow |V\rangle \rightarrow |+45\rangle \rightarrow |H\rangle$ corresponds to a *clockwise* 180° in the plane-of-polarization. Thus, the the rotation must be realized by a medium whose product $VBd = -\pi$. Consequently, the dynamic phase $\gamma = kn_0 d - \pi \cos \theta$ for the state considered in Eq. A5.

3. Overall Phase & the Circulator Attack

We have already shown that an initial state
\[|\psi\rangle = \cos(\theta/2)|R\rangle + \sin(\theta/2)|L\rangle, \tag{A10}\]

will accumulate a geometric phase $\beta = -\pi(1 - \cos \theta)$ and a dynamic phase $\gamma = kn_0 d - \pi \cos \theta$, resulting in an overall phase $\phi = kn_0 d - \pi$. Repeating this procedure for the orthogonal state
\[|\psi_\perp\rangle = -\sin(\theta/2)|R\rangle + \cos(\theta/2)|L\rangle, \tag{A11}\]

we obtain a geometric phase of $\beta' = -\beta = +\pi(1 - \cos \theta)$ and a dynamic phase $\gamma' = kn_0 d + \pi \cos \theta$, resulting in an overall phase $\phi' = kn_0 d + \pi = \phi + 2\pi$.

Let the entangled pair initially be in the Bell state $|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|HV\rangle - |VH\rangle)$. With the first qubit Alice’s photon and the second one Bob’s photon. We can rewrite the Bell state in the basis defined by Equations A10 and A11,
\[|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|HV\rangle - |VH\rangle) = \frac{i}{\sqrt{2}} \left( |\psi_\perp\rangle_A |\psi\rangle_B - |\psi\rangle_A |\psi_\perp\rangle_B \right). \tag{A12}\]

The state of the Bell pair after Bob’s photon goes through Eve’s circulator based attack, $\hat{U}_{Attack}$, is given by
\[|\Psi^-\rangle \rightarrow \hat{U}_{Attack} \frac{i}{\sqrt{2}} \left( |\psi_\perp\rangle_A |\psi\rangle_B - |\psi\rangle_A |\psi_\perp\rangle_B \right) = \frac{i}{\sqrt{2}} \left( e^{i\phi} |\psi_\perp\rangle_A |\psi\rangle_B - e^{i\phi'} |\psi\rangle_A |\psi_\perp\rangle_B \right) \tag{A13}\]
\[= i e^{i\phi} |\psi_-\rangle = -e^{i kn_0 d} |\Psi^-\rangle \tag{A14}\]

We can see from this expression, that the initial Bell state remains unchanged from the introduction of the circulators, and is equivalent to the result obtained by direct calculation in Eq. 5.

Recent work assumed that the contribution from the dynamic phase was “zero, or is known and compensated for” and predicted instead that the circulators imparted a non-local geometric phase to produce a dramatic change[15].

\[|\Psi^-\rangle \rightarrow \hat{U}_{Attack} \frac{i}{\sqrt{2}} \left( |\psi_\perp\rangle_A |\psi\rangle_B - |\psi\rangle_A |\psi_\perp\rangle_B \right) = \frac{i}{\sqrt{2}} \left( e^{i\beta} |\psi_\perp\rangle_A |\psi\rangle_B - e^{-i\beta} |\psi\rangle_A |\psi_\perp\rangle_B \right). \tag{A15}\]

However, we note that the dynamic phase (Eq. A9) is likewise non-local (due to its dependence on $\theta$) and combines with the geometric phase to produce no measurable net change in the state.