# 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 Kurtsiefer[1,2,a)]

[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, 10000 Burnet Rd, Austin, Texas 78758, USA*

[4)] *SpeQtral, 73 Science Park Drive, Singapore 118254, Singapore*

(Dated: 16 September 2019)

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 evading detection.

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[1–4]. 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[5]. Existing countermeasures[6–8] e.g. based on monitoring round-trip times have been evaded by sophisticated intercept, spoofing and delay techniques[9].

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-based quantum key distribution[10–12]. Tight time correlations between entangled photons prepared by spontaneous parametric down conversion (SPDC) allow synchronizing independent atomic clocks at photon rates of order 100 pairs/s[10] and with potential accuracies $< 1\,\mathrm{ps}$[11]. Monogamy of entanglement ensures that a counterfeit photon entangled with the legitimate signal cannot be generated, allowing signal authentication[13]. The no-cloning theorem prevents intercept, copy and resend of an identical quantum state with an arbitrary delay[14].

Despite these security enhancements, the vulnerability to an asymmetric delay attack remains since photons traveling in opposite directions can be passively rerouted with a circulator (Figure 1) by using the Faraday effect

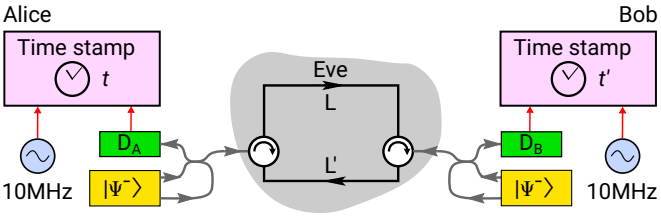


FIG. 1. Clock synchronization scheme. Alice and Bob each have a source of polarization-entangled photon pairs $|\Psi^-\rangle$, and avalanche photodetectors at $\mathrm{D_{A,B}}$. One photon of the pair is detected locally, while the other photon is sent through a fiber to be detected on the remote side. 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.

to break the reciprocity of the channel. A recent proposal suggests that even polarization-insensitive circulators, which rotate input polarizations back to the same state, impose a measurable change in the phase of the joint state[15]. The proposal was based on the fact that the phase change after a cyclic quantum evolution is measurable under certain conditions[16]. Previous experiments with entangled photons[17–20] seemed to support this proposed protection.

In this work, we examine the circulator-based asymmetric delay attack[15]. We experimentally show that the attack *cannot* be detected by the proposed mechanism and demonstrate an induced error in synchronization of over 25 ns between two rubidium clocks.

We briefly review the clock synchronization protocol considered[15]. The protocol involves two parties, Alice

[a)] Electronic mail: christian.kurtsiefer@gmail.com

and Bob, connected by a single mode optical channel. Each party has a source of polarization-entangled photons 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 $t$ and $t'$.

Photon pairs emerging from SPDC are tightly time-correlated. Thus, for an offset $\delta$ 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

$$\tau_{AB} = \delta + \Delta t_{AB} \quad \text{and} \quad \tau_{BA} = \delta - \Delta t_{BA} \tag{1}$$

due to pairs created by Alice and Bob[21]. A round-trip time $\Delta T$ for photons can be calculated using the inter-peak separation,

$$\Delta T = \Delta t_{AB} + \Delta t_{BA} = \tau_{AB} - \tau_{BA}, \tag{2}$$

while the offset

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

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

$$\delta = \frac{1}{2}\left(\tau_{AB} + \tau_{BA}\right) \tag{4}$$

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 ($\mathrm{D_{A,B}}$). 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 ($|\psi\rangle_B \to \pm|\psi\rangle_B$) does not result in any measurable change

$$|\Psi^-\rangle \to \pm\frac{1}{\sqrt{2}}(|HV\rangle - |VH\rangle) = \pm|\Psi^-\rangle. \tag{5}$$

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[16] – 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). In subsequent sections, we use this result to experimentally demonstrate an asymmetric delay attack which evades detection.

*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 ≈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 $\mu$m into a 2 mm thick $\beta$-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 $\mathrm{s^{-1}}$. Fiber beam splitters separate the photon pairs so that one photon is detected locally with an avalanche photodetector ($\mathrm{D_{A,B}}$), 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 ≈ 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.

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 $L'$.

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 $L$

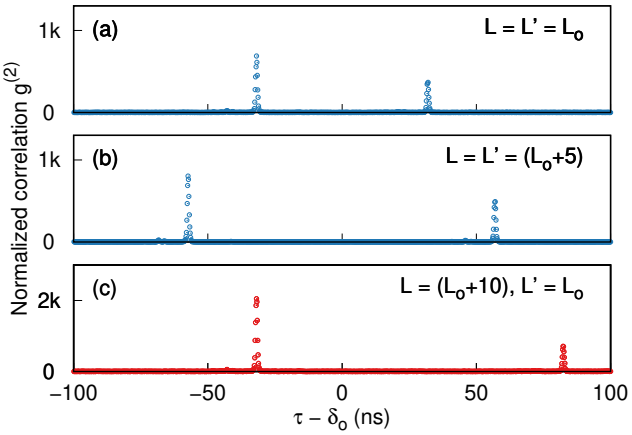


FIG. 2. Time correlations of Alice and Bob's detection events normalized to background coincidences. The separation between peaks corresponds to the round-trip time $\Delta T$, and the midpoint is the offset between the clocks $\delta$. Symmetric delays with $L = L'$ show that the offset remains constant for both the (a) initial and (b) extended round-trip times. An asymmetric delay with (c) $L = L' + 10$ results in an offset shift. $L_o/2$: minimum length of the fiber belonging to each circulator port. $\delta_o$: the offset estimated in (a).

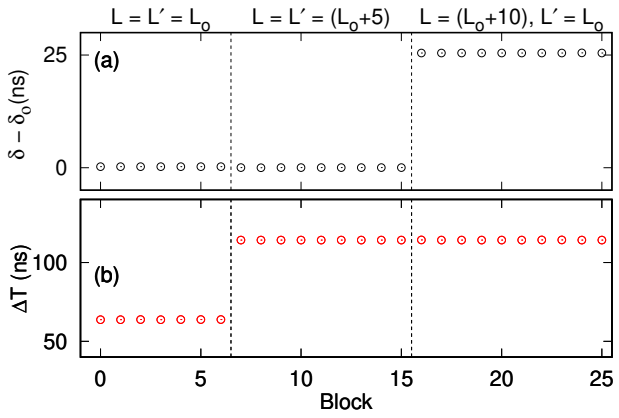


FIG. 3. (a) Measured offset $\delta$ between two clocks, both locked on the same frequency reference. Each value of $\delta$ was evaluated from measuring photon pair timing correlations from a block of photodetection times recorded by Alice and Bob. Each block is 40 s long. (b) The round-trip time $\Delta T$. Block 6 to 7: increasing the symmetric delay ($L = L'$) does not change $\delta$. Block 15 to 16: introducing an asymmetric delay ($L \neq L'$) creates an offset error. The delay was created by redistributing the additional delays in Blocks 7 to 15, so that $\Delta T$ remains the same. $\delta_o$: offset measured in the first block.

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.

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 horizontal, vertical, diagonal (+45°), anti-diagonal (−45°), left-circular, or right-circular polarization ($|H\rangle, |V\rangle, |D\rangle, |A\rangle, |L\rangle$ 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[24].

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

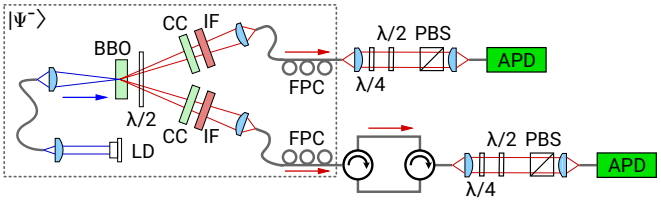


FIG. 4. Setup for quantum state tomography on a polarization-entangled photon pair state, with one photon passing through a pair of circulators. Dashed box: optical setup of our polarization-entangled photon source[22]. LD: laser diode, BBO: $\beta$-Barium Borate, CC: compensation crystals, FPC: fiber polarization controller, SMF: single mode fiber, $\lambda/4$: quarter-wave plate, $\lambda/2$: half-wave plate, PBS: polarizing beam splitter, APD: avalanche photodiode.

compare $\rho_o$ and $\rho$ by computing the fidelity $F(\rho, \rho_o) = \left(\mathrm{Tr}\sqrt{\sqrt{\rho}\rho_o\sqrt{\rho}}\right)^2$. 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[24]. 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-

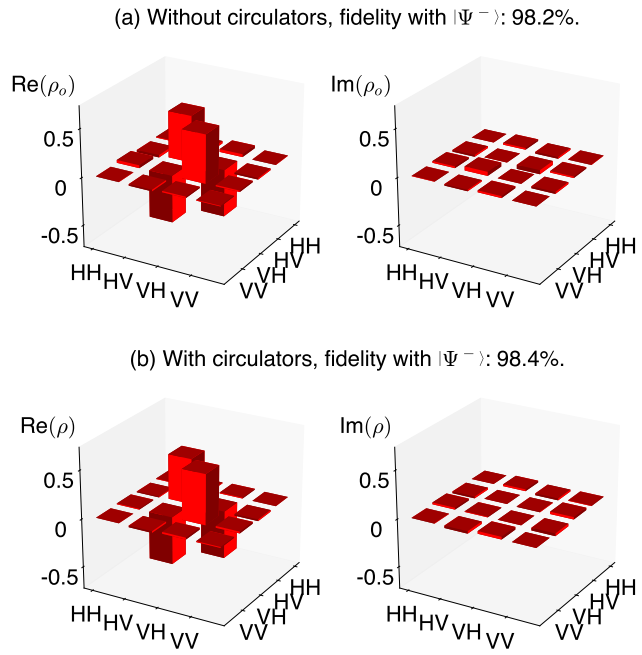


FIG. 5. Real and imaginary part of the reconstructed density matrix for the target Bell state $|\Psi^-\rangle$ originating from Alice's source. Bob receives one photon of the pair through the synchronization channel. The density matrices obtained (a) without and (b) with polarization-insensitive circulators in the line (Figure 4) do not deviate significantly from $|\Psi^-\rangle$.

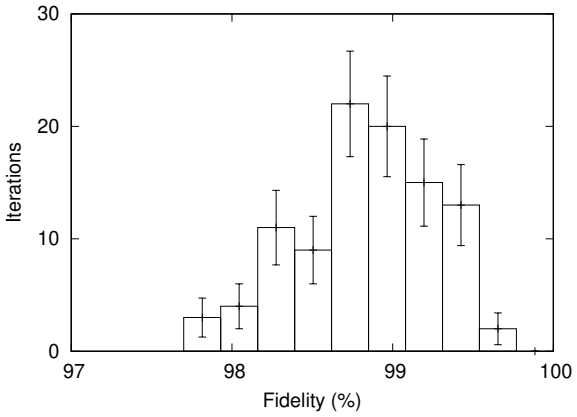


FIG. 6. Fidelity distribution comparing the Bell state originating from Alice's source before and after introducing the circulators. The distribution is generated by numerically propagating errors due to counting statistics. A high mean fidelity suggests that the state remains unchanged and cannot be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

unity value of $F$, we conclude that the circulators do not affect the distributed Bell state.

*Conclusion* – We have 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[5]. 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[25–29] and quantum non-demolition measurements[12] 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.

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.

*Supplementary Material* – In the supplementary material, we examine the geometric phase associated with polarization state rotation in the circulators, previously thought to be observable[15]. We show that an additional phase, associated with photon dynamics in the Faraday Rotator, neutralizes this geometric phase.

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.

[1] D. L. Mills, IEEE Transactions on Communications **39**, 1482 (1991).
[2] IEC 61588:2009(E) , C1 (2009).
[3] D. Piester, A. Bauch, L. Breakiron, D. Matsakis, B. Blanzano, and O. Koudelka, Metrologia **45**, 185 (2008).
[4] Z. Jiang, Y. Huan, V. Zhang, and P. Dirk, *BIPM 2017 TWSTFT SATRE/SDR calibrations for UTC and Non-UTC links*, Tech. Rep. (BIPM Technical Memorandum, TM268 V2a, 2017).
[5] L. Narula and T. E. Humphreys, IEEE Journal of Selected Topics in Signal Processing **12**, 749 (2018).
[6] T. Mizrahi, in *2012 IEEE International Symposium on Precision Clock Synchronization for Measurement, Control and Communication Proceedings* (IEEE, 2012) pp. 1–6.
[7] M. Ullmann and M. Vögeler, in *2009 International Symposium*

*on Precision Clock Synchronization for Measurement, Control and Communication* (IEEE, 2009) pp. 1–6.
[8] J. Tsang and K. Beznosov, in *International Conference on Information and Communications Security* (Springer, 2006) pp. 50–59.
[9] D. Rabadi, R. Tan, D. K. Yau, and S. Viswanathan, in *Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security* (ACM, 2017) pp. 874–886.
[10] J. Lee, L. Shen, A. Cerè, J. Troupe, A. Lamas-Linares, and C. Kurtsiefer, Applied Physics Letters **114**, 101102 (2019).
[11] F. Hou, R. Quan, R. Dong, X. Xiang, B. Li, T. Liu, X. Yang, H. Li, L. You, Z. Wang, and S. Zhang, Phys. Rev. A **100**, 023849 (2019).
[12] A. Lamas-Linares and J. Troupe, in *Advances in Photonics of Quantum Computing, Memory, and Communication XI*, Vol. 10547 (International Society for Optics and Photonics, 2018) p. 105470L.
[13] D. Yang, Physics Letters A **360**, 249 (2006).
[14] W. K. Wootters and W. H. Zurek, Nature **299**, 802 (1982).
[15] J. E. Troupe and A. Lamas-Linares, arXiv preprint arXiv:1808.09019 (2018).
[16] M. V. Berry, Journal of Modern Optics **34**, 1401 (1987).
[17] P. G. Kwiat and R. Y. Chiao, Physical Review Letters **66**, 588 (1991).
[18] D. V. Strekalov and Y. H. Shih, Physical Review A **56**, 3129 (1997).
[19] J. Brendel, W. Dultz, and W. Martinessen, Physical Review A **52**, 2551 (1995).
[20] A. K. Jha, M. Malik, and R. W. Boyd, Physical Review Letters **101**, 180405 (2009).
[21] R. J. Glauber, Physical Review **130**, 2529 (1963).
[22] P. G. Kwiat, K. Mattle, H. Weinfurter, A. Zeilinger, A. V. Sergienko, and Y. Shih, Phys. Rev. Lett. **75**, 4337 (1995).
[23] C. Ho, A. Lamas-Linares, and C. Kurtsiefer, New Journal of Physics **11**, 045011 (2009).
[24] J. B. Altepeter, E. R. Jeffrey, and P. G. Kwiat, Advances in Atomic, Molecular, and Optical Physics **52**, 105 (2005).
[25] D. Jalas, A. Y. Petrov, and M. Eich, Optics letters **39**, 1425 (2014).
[26] V. Dmitriev, G. Portela, and D. Zimmer, Optics letters **38**, 4040 (2013).
[27] V. Dmitriev, M. N. Kawakatsu, and G. Portela, Optics letters **38**, 1016 (2013).
[28] L. Bi, J. Hu, P. Jiang, D. H. Kim, G. F. Dionne, L. C. Kimerling, and C. Ross, Nature Photonics **5**, 758 (2011).
[29] Z. Yu and S. Fan, Nature photonics **3**, 91 (2009).
[30] J. Anandan, Nature **360**, 307 (1992).
[31] J. Zak, Physics Letters A **154**, 471 (1991).