Clock synchronization by remote detection of correlated photon pairs

New Journal of Physics
The open-access journal for physics

Clock synchronization by remote detection of correlated photon pairs

Caleb Ho[1], **Antía Lamas-Linares**[1,2] **and Christian Kurtsiefer**[1,2,3]
[1] Centre for Quantum Technologies, National University of Singapore, 3 Science Drive 2, 117543, Singapore
[2] Department of Physics, National University of Singapore, 2 Science Drive 3, 117542, Singapore
E-mail: christian.kurtsiefer@gmail.com

New Journal of Physics **11** (2009) 045011 (13pp)
Received 21 January 2009
Published 30 April 2009
Online at http://www.njp.org/
doi:10.1088/1367-2630/11/4/045011

Abstract. In this study, we present an algorithm to detect the time and frequency differences of independent clocks based on observation of time-correlated photon pairs. This enables remote coincidence identification in entanglement-based quantum key distribution schemes without dedicated coincidence hardware, pulsed sources with a timing structure or very stable reference clocks. We discuss the method for typical operating conditions and show that the requirement for reference clock accuracy can be relaxed by about five orders of magnitude in comparison with previous schemes.

[3] Author to whom any correspondence should be addressed.

Contents

1. Introduction 2
2. Photon pair identification with remote clocks 3
3. Finding the time offset 4
4. Finding the time offset in the presence of a frequency difference 7
5. Iterative procedure to decrease timing and frequency uncertainty 9
6. A faster algorithm for finding the fine time offset 10
7. Conclusion 11
Acknowledgments 12
Appendix. Iterative algorithm for finding time and frequency differences 12
References 13

1. Introduction

Quantum key distribution (QKD) [1]–[3] is the only quantum information protocol that has found its way into practical applications, and is currently in a stage of early commercial development. There are two families of protocols that use fundamentally different resources. The original QKD protocol BB84 [4] and its variants transmit single photons (or approximations thereof), while the other family [5] performs measurements on pairs of entangled photons. A few years ago, entanglement-based QKD protocols were viewed as equivalent to BB84 [6], and thus only of little interest for practical QKD due to their additional complexity. The new concept of device-independent QKD [7], and a returned awareness of classical side channels in prepare-and-send protocols revived interest in entanglement-based QKD schemes. Entangled photon pairs are efficiently prepared by spontaneous parametric down conversion (SPDC). Demonstrated for polarization-entangled pairs in 1995 [8], recent developments led to the extremely bright sources available today [9, 10], so that entanglement-based QKD became a viable option.

The first step in establishing a key in such a scheme is the assignment of photodetection events to entangled photon pairs. Due to their strong temporal correlation (down to a few hundred femtoseconds) in typical pair sources [11], this assignment can be done via temporal coincidence identification. In typical laboratory experiments, as well as in early QKD implementations, a hardware channel was used to carry out this coincidence identification [12, 13]. Less hardware is required when coincidences are identified by comparing detection times given by good local clocks [14, 15] or a central time reference broadcast by the Global Positioning System [16].

In this paper, we present an algorithm that relaxes the rather stringent reference clock quality requirements for such a coincidence identification so that conventional crystal oscillators can be used. In section 2, we outline the general problem and present a robust coincidence tracking scheme. Section 3 covers the algorithm to find an initial time offset as implemented in earlier experiments [15, 17]. In sections 4–6, we extend this scheme in the presence of a frequency difference between the clocks necessary to permit the use of clocks with lower accuracy.

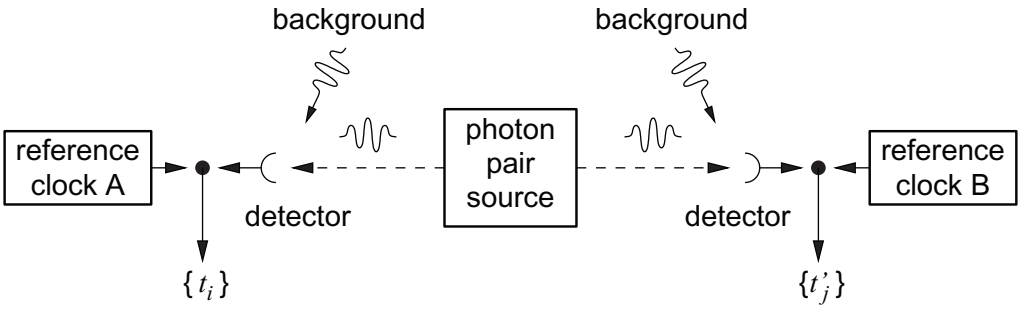

Figure 1. Setting of the problem. Detection times of photoevents from a correlated photon pair source and background are registered with respect to two local reference clocks at remote locations A and B. The true coincidences need then to be identified from the time sets $\{t_i\}$ and $\{t'_j\}$ on both sides.

2. Photon pair identification with remote clocks

The identification of pairs is straightforward in any context in which a hardware coincidence gate can be used; this is the case in laboratory-based experiments or field setups with a dedicated synchronization channel.

The situation we address in this paper applies to cases where detection times of photons at the two distant locations [15, 16, 18] are recorded, and coincidences are identified based on these time stamps (see figure 1). This method requires stable and synchronous clocks to be used for the time stamping: a typical coincidence window τ_c is chosen to be slightly larger than the detector time jitter, which is of the order of 1 ns. The data acquisition for establishing a key out of measurements is supposed to run either continuously, or at least for a few hundred seconds. To maintain two clocks synchronized within τ_c after a time of 100 s, a relative accuracy of 10^{-11} is required, a specification that is met by commercial rubidium clocks. For longer operation times, this still may be insufficient unless either a timing signal is transmitted on a separate channel, or the time reference is provided by a central source.

Pair sources based on SPDC provide enough information in the streams of photodetection times $\{t_i\}$ and $\{t'_j\}$ that such accurate clocks should not be necessary. As long as the pair events are initially identified, the drift of the clocks can be tracked directly from the coincidence signal. For this to work reliably, the rate of pair events must be significantly larger than the one for accidental coincidences due to background photons in the same time window τ_c, which is also a necessary condition for a obtaining a secure key in QKD.

In its simplest form, a floating average of the time difference $\Delta t = t_i - t'_j$ between true coincidence events can be used to track a drift of the reference time between the two sides. To illustrate this, and to evaluate the intrinsic clock stability necessary to follow the coincidence signature, we consider a realistic situation where the full-width at half-maximum of a coincidence time distribution due to detector jitter is $\tau_d = 1$ ns. To estimate the center of this distribution with an uncertainty (one standard deviation) of $\delta\tau = 0.1$ ns, we need to average time differences over about

$$n = \left(\frac{\tau_d}{2\sqrt{2\ln 2}\delta\tau}\right)^2 + 1 \approx 19 \tag{1}$$

coincidence events. Even for very low coincidence detection rates of 100 counts per second (cps), it takes less than 0.2 s to get a sufficient number of events. Over that period, the clock should not drift such that an event leaves the coincidence window, which translates into a relative frequency *accuracy* requirement of 10^{-8} over 100 ms. More realistic coincidence detection rates of 1–10 kcps require only a relative frequency accuracy of 10^{-7} to 10^{-6} over a period of 1–10 ms. Standard crystal oscillators easily exhibit a *stability* of that order, but may lack the accuracy. Thus, tracking the time difference in coincidences from a set of detection events permits these simpler reference oscillators to be used during normal operation.

Two problems are left for recovering the coincidences from time stamps derived with respect to two separate clocks: first, the detection instances at both sides will have an unknown time offset ΔT between them. This is mainly due to the absence of a common origin of time with a high enough resolution and propagation over the physical distance between the two sides. As long as the two reference clocks have the same frequency, ΔT can be found by looking at the cross correlation between the two timing signals. We will elaborate this in the next section.

The second problem is related to the relative frequency difference between the two clocks due to lack of accuracy. This is harder to solve, since the stream of time stamps $\{t_i\}$ and $\{t'_j\}$ on each side has no intrinsic time structure: both signal and background events follow a Poisson distribution[4].

The two problems of finding time and frequency differences from coincidence signals in the presence of uncorrelated background events are illustrated in figure 2. Figure 2(a) shows a distribution of detection events $\{t_i\}$ on side A, figure 2(b) reflects the event stream on side B, assuming that there is only a time offset ΔT, but no frequency difference between the two reference clocks. Figure 2(c) shows an event stream on side B both under the presence of a time offset and a frequency difference. For convenience, we describe the relative frequency difference by a quantity Δu, such that the detection times t, t' on both sides due to identified photon pairs are connected via

$$t' = (t + \Delta T) \cdot (1 + \Delta u). \tag{2}$$

We now estimate how accurately ΔT and Δu need to be determined. In a practical QKD implementation, the two time stamping clocks are coarsely synchronized with conventional means (e.g. using the network timing protocol [20]), so it can be assumed that ΔT will not exceed a few hundred milliseconds. A coincidence time window may be about 1–5 ns wide, fixing the uncertainty in ΔT to be small enough to start coincidence time tracking as sketched above. Thus, ΔT needs to be known with a precision of a few 10^{-9}, corresponding to an information of about 26–28 bits. For the tracking algorithm to take over, the relative frequency difference Δu also needs to be known to an uncertainty of 10^{-8} to 10^{-6}. An upper bound for $|\Delta u|$ can be chosen to match a typical accuracy of standard crystal oscillators (e.g. 10^{-4}). Thus, Δu of the two clocks needs to be found with a precision of 10^{-2} to 10^{-4}, equivalent to an information of 7–14 bits.

3. Finding the time offset

We first explain the algorithm to find the time offset ΔT, assuming that the two reference clocks run at the same frequency ($\Delta u = 0$). Two streams of detection events $\{t_i\}$ and $\{t'_j\}$ on both sides

[4] While it has been shown that the light emerging from SPDC processes should exhibit super-Poissonian statistics [19], this is typically not observed in practical SPDC systems with photon counting detectors because it is washed out by multi-mode effects on a timescale way below the detector resolution.

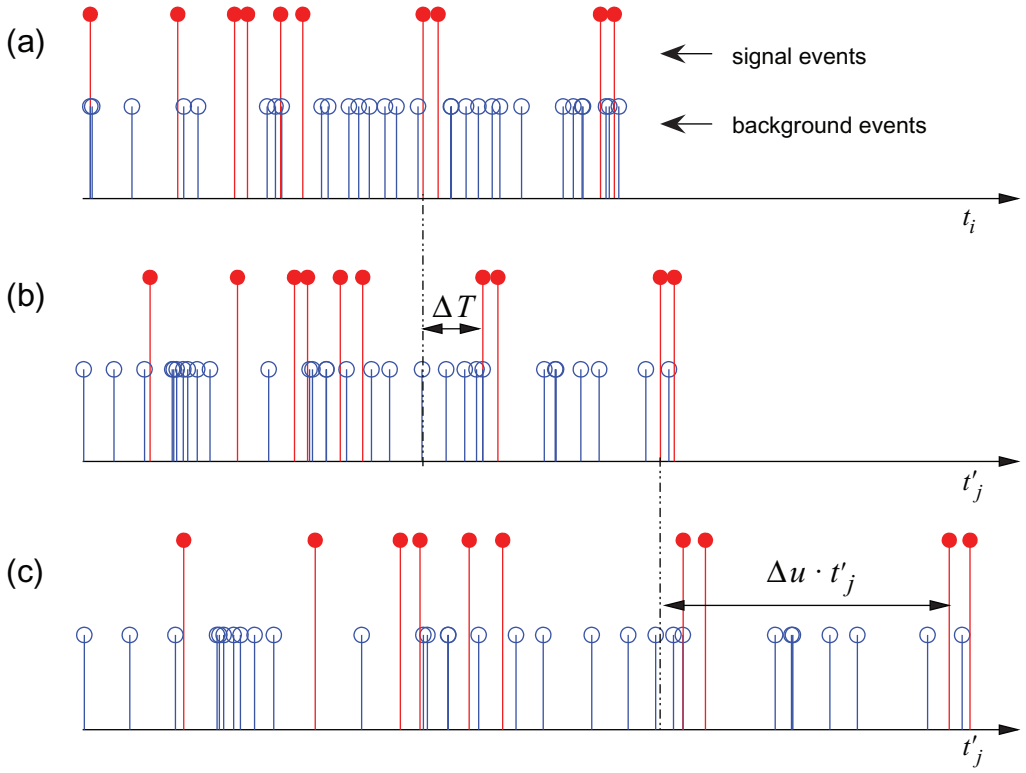

Figure 2. Effect of time offset and clock drift on photoevent sets. Panel (a) represents the event set $\{t_i\}$ on side A, panel (b) an event set $\{t'_j\}$ on side B with a time offset ΔT, but the same reference clock frequency. Panel (c) illustrates a set $\{t'_j\}$ with an additional relative frequency difference Δu between both reference clocks.

are translated into detection time functions

$$a(t) = \sum_i \delta(t - t_i), \qquad b(t) = \sum_j \delta(t - t'_j)\,. \tag{3}$$

The cross correlation between these two functions,

$$c(\tau) = (a \star b)(\tau) := \int a(t)b(t+\tau)\,\mathrm{d}t\,, \tag{4}$$

has a peak at $\tau = \Delta T$ due to the correlated photodetection events on top of an unstructured but noisy baseline from independent background detection events on both sides. The time offset ΔT is thus simply found by searching for the maximum in $c(\tau)$. In practice, $c(\tau)$ is efficiently obtained from the timing sets via fast Fourier transformations (FFTs) and their inverse,

$$c(\tau) = \mathcal{F}^{-1}\left[\mathcal{F}^*[a] \cdot \mathcal{F}[b]\right]\,, \tag{5}$$

with discrete arrays for a, b and c of length N (typically a power of 2). The high resolution necessary for ΔT (28 bits) renders a direct calculation impractical. It is possible, however, to obtain the coarse and fine part of ΔT separately with much smaller sample sizes. To illustrate how this works, we take the timing events $\{t_i\}$ and $\{t'_j\}$ captured during an acquisition time T_a,

Table 1. Connection between the probability ϵ of wrong peak identification, bin number N and statistical significance S of a peak.

ϵ/N	10^{-4}	10^{-5}	10^{-6}	10^{-7}	10^{-8}	10^{-9}	10^{-10}	10^{-11}	10^{-12}
S	3.72	4.26	4.75	5.12	5.61	6.00	6.36	6.71	7.03

and map them onto the discrete arrays $\{a_k\}$ and $\{b_k\}$ with a time resolution δt:

$$a_k = \sum_i \delta_{k,\lfloor (t_i/\delta t) \bmod \mathrm{N} \rfloor}, \qquad k = 0, \ldots, N-1\,, \tag{6}$$

and $\{b_k\}$ accordingly. This is an efficient process, which requires visiting each entry t_i only once. The cross correlation array $\{c_k\}$ is obtained by the discrete version of equation (5), and its maximum obtained by a subsequent linear search in $\{c_k\}$. If the cross correlation peak can be identified correctly, the result $k_{\max}$ reflects ΔT up to a resolution δt and modulo $N\delta t$. Thus, applying this method with two different resolutions δt leads to a final ΔT with a resolution of 26–28 bits, while the individual FFTs are carried out at a moderate size of $N = 2^{19}$ or less. The complete code for this procedure is available as open source[5].

It is beneficial to consider the influence of uncorrelated background events in this peak finding process. We assume a signal rate r_s of true coincidences, and background rates r_1 and r_2 on both sides. The discrete arrays $\{a_k\}$ and $\{b_k\}$ are built up from time stamps $\{t_i\}$ and $\{t'_j\}$ in a collection interval T_a. The cross correlation peak will be made up by $r_\mathrm{s}T_\mathrm{a}$ event pairs at the index $k_{\max}$, while the $r_1 r_2 T_\mathrm{a}^2$ background event pairs are homogeneously distributed over all N entries in $\{c_k\}$ following a Poisson distribution. The peak can be identified with sufficient confidence if its statistical significance S, here defined as the ratio between the peak height above the baseline and the standard deviation of the latter,

$$S(k) := \frac{c_k - \overline{c_k}}{\sqrt{\overline{(c_k - \overline{c_k})^2}}}\,, \tag{7}$$

exceeds a certain numerical value. With the above rates, the peak value arising from signal pairs is

$$S_\mathrm{p} = \frac{r_\mathrm{s}T_\mathrm{a}}{\sqrt{r_1 r_2 T_\mathrm{a}^2/N}} = \sqrt{\frac{r_\mathrm{s}^2 N}{r_1 r_2}}\,. \tag{8}$$

If we approximate the fluctuations on the baseline of $\{c_k\}$ by a Gaussian distribution, the probability ϵ that a baseline fluctuation gives rise to the largest value $S_{\max}$, and thus leads to a wrongly identified location of the cross correlation peak, is given by

$$\epsilon = \mathcal{P}\left(S_{\max} > S_\mathrm{p}\right) \approx \frac{N}{2}\left(1 - \operatorname{erf}\frac{S_\mathrm{p}}{\sqrt{2}}\right)\,. \tag{9}$$

A numerical evaluation of this quantity (see table 1) shows that for $N < 10^7$, $S_\mathrm{p} > 6$ leaves less than 1% probability of misidentifying the peak. Since $S_{\max}$ can be directly estimated out of $\{c_k\}$, it forms a good basis to gauge the success of the peak finding procedure in practice.

[5] The code is available from http://code.google.com/p/qcrypto.

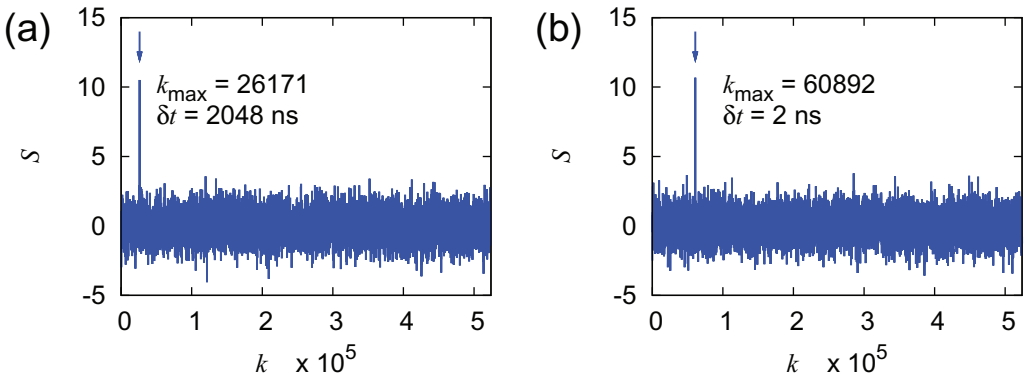

Figure 3. Cross correlation arrays $\{c_k\}$ of photoevents acquired over $T_a \approx 1.05$ s, normalized to a statistical significance S as defined in equation (7) with $N = 2^{19}$. The k_{max} for two time resolutions δt in (a) and (b) lead to a value $\Delta T = 53\,599\,160 \pm 2$ ns. All traces are sampled down by a factor 64.

Care should be taken that events acquired over a time T_a are uniformly distributed over the interval $N\delta t$ in the binning procedure of equation (6). Specifically, $T_a/(N\delta t)$ should be an integer number. Otherwise, uncorrelated background events are subject to an effective envelope and do not lead to a flat baseline in the cross correlation array, so determination of $\overline{c_k}$ and subsequent peak finding becomes difficult. This problem can also be addressed by removing the lowest Fourier components in equation (5) before the back transformation.

From equation (8) it can be seen that for given rates r_1, r_2 and r_s, the only way to increase the success probability is to increase the number of time bins N. For $r_1 = r_2 = 100$ kcps, r_s=1 kcps, we need $N \approx 360\,000 < 2^{19}$ to exceed $S = 6$. Furthermore, the frequency difference of the reference clocks needs to be very small. A time stretch $T_a \Delta u$ between the two clocks over an acquisition time T_a exceeding the targeted resolution δt for ΔT reduces the statistical significance of the coincidence peak below a useful level. With parameters $\delta t = 2$ ns and T_a of a few seconds for the experiments carried out in [15, 17], reference clocks with a relative frequency difference $\Delta u < 10^{-9}$ were necessary, which were provided in the form of rubidium oscillators.

Figure 3 shows the result of typical correlation arrays $\{c_k\}$ (rescaled in terms of S) from an experiment with event rates $r_1 \approx 68$ kcps, $r_2 \approx 56$ kcps and $r_s \approx 1280$ cps. Here, $N = 2^{19}$ was chosen, and time resolutions $\delta t = 2048$ ns for the coarse and $\delta t = 2$ ns for the fine resolution. The peak exhibits $S > 10$ for both resolutions and the resulting time offset is $\Delta T = 53\,599\,160 \pm 2$ ns.

4. Finding the time offset in the presence of a frequency difference

The only reason to use reference clocks with a relative frequency accuracy better than 10^{-9} with the presented algorithms is to determine the initial time offset ΔT with a resolution of the order of 1 ns. Knowledge of the frequency difference to that accuracy and a reasonable stability is sufficient for tracking, so it is desirable to extract this information out of the timing events efficiently.

Finding both the time and frequency differences from the recorded timing signals $\{t_i\}$ and $\{t'_j\}$ in the presence of uncorrelated background events is equivalent of identifying a line in a (t_i, t'_k) plane of all possible pair events. This well-known pattern recognition problem is formally solved by the Hough transformation [21], which maps the pair time distribution $\{(t_i, t'_k)\}$ onto the parameter space $\{(\Delta T, \Delta u)\}$. As in the cross correlation method in the previous section, the pair $(\Delta T, \Delta u)$ searched for is the peak coordinate in the parameter space. However, we did not find an equally efficient high-resolution solution as for the one-dimensional problem in section 3.

A simpler method for determining Δu is to estimate time offsets ΔT_1 and ΔT_2 during relatively short acquisition intervals T_a, shifted by a time $T_s > T_a$ with the method described in the previous section. The change in time offsets between these probe intervals is connected with the relative frequency difference Δu via

$$\Delta u = \frac{\Delta T_1 - \Delta T_2}{T_s}. \tag{10}$$

However, it is necessary to reliably obtain the time offsets on the two sampling intervals—which itself is only possible with clocks with a sufficiently small Δu. We now evaluate under which conditions this cross correlation step will succeed in finding a time offset ΔT.

For two clocks with $\Delta u = 0$, the contribution of correlated events will all end up in a single time bin in the discrete correlation array $\{c_k\}$. For $\Delta u \neq 0$, the correlated events will spread out over roughly $m = \Delta u T_a/\delta t$ bin indices k. This reduces not only the statistical significance S for identifying a maximum, but also increases a timing uncertainty which in turn leads to an uncertainty in determining the frequency difference Δu according to equation (10).

In order to identify the correlation peak with sufficient confidence $1 - \epsilon$ according to equation (9), the statistical significance should exceed a threshold $S_{th} \approx 6$. For this, the timing resolution δt may have to be increased, forcing the true coincidences in fewer bins k, up to $\delta t = \Delta u T_a$, or equivalently $N = 1/\Delta u$. This, together with equation (8) for the statistical significance, leads to an expression for the maximally acceptable frequency difference

$$\Delta u_{max} = \frac{r_s^2}{r_1 r_2 S_{th}^2} \tag{11}$$

for this strategy. In practice, the choice of a suitable size N for the correlation array $\{c_j\}$ does not have to be done before the time-consuming step of the cross correlation in equation (5). If with an initially chosen resolution δt the peak is not found, the array $\{c_j\}$ can be either re-partitioned in larger bins of width $\delta t'$, or equivalently exposed to a moving average procedure until a statistically significant correlation peak is identified. Once the time offset ΔT is known with an accuracy $\delta t'$, the relative frequency difference Δu is known with an accuracy

$$\delta u \approx \sqrt{2}\frac{\delta t'}{T_s} = \sqrt{2}\frac{T_a}{N T_s}. \tag{12}$$

We illustrate this method with experimental timing sets obtained from a non-optimized down conversion source with moderate background event rates ($r_1 \approx r_2 \approx 77$ kcps, $r_s \approx 15$ kcps). Both time stamp units were referenced to crystal oscillators with a nominal frequency accuracy of 100 ppm.

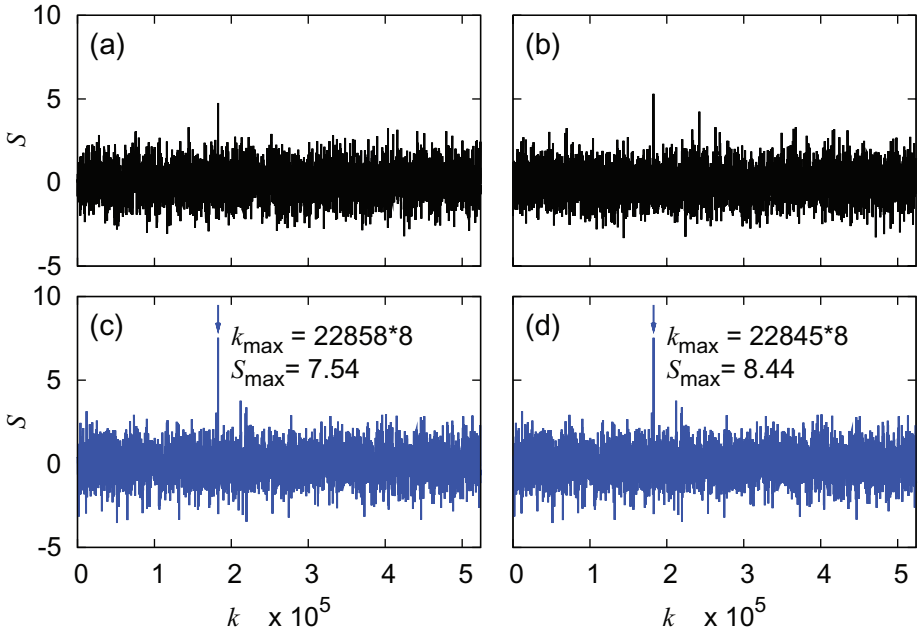

Figure 4. Correlation arrays for photoevents acquired with slightly detuned reference clocks. Panels (a) and (b) show arrays taken during acquisition time slots $T_a \approx 268$ ms (1 s for events at side B), separated by $T_s \approx 1.074$ s and $\delta t = 2.048\,\mu$s—correlation peaks cannot be identified with sufficient significance. Panels (c) and (d) show the arrays after summing every eight adjacent bins, revealing a moving correlation peak. All traces are sampled down.

With two segments of $T_a = 2^{28}$ ns ≈ 268 ms and a separation of $T_s = 4T_a \approx 1.074$ s, convolution arrays $\{c_k\}$ were generated with a binning resolution of $\delta t = 2.048\,\mu$s. Since there were slowly varying changes in the background rates, the 20 lowest frequency entries (and their mirrors) were set to 0 before back transformation to $\{c_k\}$, resulting in a smooth baseline. The results are shown in the top panels of figure 4, without any significant correlation peaks. A subsequent re-binning with an effective width of $\delta t' = 16.384\,\mu$s reduced the noise level of the background sufficiently to allow the identification of the correlation peaks, resulting in time offsets of $\Delta T_1 = \Delta T = 374\,505 \pm 16\,\mu$s, $\Delta T_2 = 374\,292 \pm 16\,\mu$s and subsequently in $\Delta u = (1.98 \pm 0.21) \times 10^{-4}$.

5. Iterative procedure to decrease timing and frequency uncertainty

A simple method for obtaining both ΔT and Δu by analyzing correlations typically does not provide a sufficiently low uncertainty to start the tracking algorithm described in section 2. Therefore, additional steps are required. Knowledge of Δu with uncertainty $\delta u < \Delta u$, the linear dependency of the timing uncertainty δt from Δu according to equation (12) and the time offset ΔT with some accuracy suggests an iterative method for this purpose.

A set $\{\tilde{t}'_j\}$ is prepared from $\{t'_j\}$, which is corrected with the initial values ΔT and Δu (obtained as in section 4) via

$$\tilde{t}'_j = (\tilde{t}'_j + \Delta T) \cdot (1 + \Delta u). \tag{13}$$

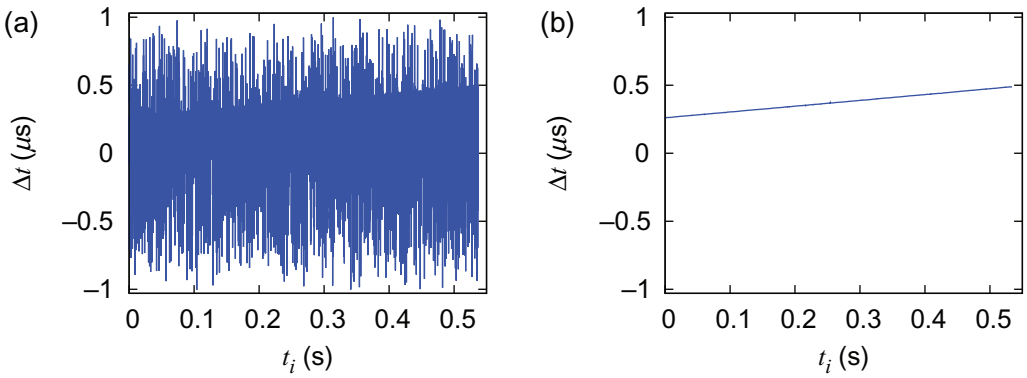

Figure 5. (a) Time differences Δt between event pairs on both sides falling into the same time bin after pre-compensation with approximate $\Delta T, \Delta u$. A large fraction of the pairs appear on a line, with accidental coincidental pairs contributing to the noise of the figure. The differences fall in the range $\pm\delta t/2$, and are known with a high precision. (b) Dropping adjacent pairs with excessive differences leaves a line which can be used to extract the final ΔT, Δu.

With this set and the original set $\{t_i\}$, new values for Δu and ΔT are obtained. The reduction in uncertainty δu is given by the ratio $T_\mathrm{s}/T_\mathrm{a}$ according to equation (12), and is somewhat below an order of magnitude, or about three bits. This can be iterated, finally leading to values ΔT and Δu with the targeted uncertainties (see the appendix for the explicit algorithm).

6. A faster algorithm for finding the fine time offset

The iterative method in jointly finding ΔT and Δu with sufficient accuracy converges only slowly because the time separation T_s is typically not very much larger than an acquisition time interval T_a, to keep the initial time for finding the coincidences low.

Once initial values for Δu and ΔT are found, an alternative algorithm can be used: we begin with event pairs sets $\{t_i\}$ and $\{\tilde{t}'_j\}$, where the latter is corrected via equation (13) similarly as before. If the timing resolution δt for discretization is small enough (i.e. $r_{1,2}\delta t < 1$), the arrays $\{a_i\}$ and $\{b_j\}$ are only sparsely populated. For $\tilde{t}'_j \in [0, T_b]$ with $T_b = \delta t/\delta u$, signal events lead to coincidences in time bins with the same time bin indices $k = k'$. The sparse population of the arrays $\{a_k\}$ and $\{b_{k'}\}$ ensures then that the presence of a condition $a_k = b_{k'=k} = 1$ is very likely due to a true coincidence. For those pair events, the instantaneous time difference $\Delta t = t_i - \tilde{t}'_j$ due to an inaccurately known ΔT and Δu can be determined with an accuracy limited only by the time resolution of the detection system (typically dominated by detector timing jitter). Analysis of instantaneous time differences Δt over the time interval T_b finally reveals the parameters ΔT and Δu with the intrinsic resolution of the system, after which the tracking algorithm can take over.

A distribution of time differences generated with this method from the time stamps used in section 4 is shown in figure 5(a). With one more iteration of the correlation algorithm, values $\Delta T = 374\,592.8 \pm 1.0\,\mu\mathrm{s}$ and $\Delta u = 2.0123 \pm 0.0014 \times 10^{-4}$ were obtained to prepare the corrected set $\{\tilde{t}'_j\}$. The binning window for identifying coincidences was chosen as $\delta t = 1.024\,\mu\mathrm{s}$. Out of the 2^{19} bins for both sets $\{t_i\}$ and $\{\tilde{t}'_j\}$, about 41 000 were occupied with

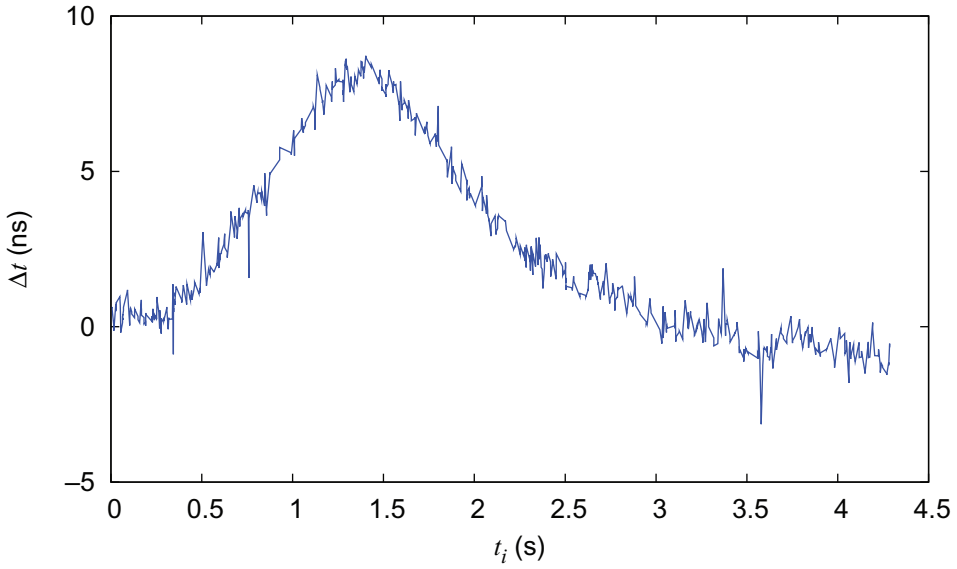

Figure 6. Time differences for coincidences after correction of the event times at side B with Δu, ΔT. The variation can now be followed by a coincidence-tracking scheme described in section 2.

one entry, and 154 and 381 with two events each; the rest were empty, thus forming sparse arrays.

One can visually identify a line structure, starting at about $+0.25\delta t$, and increasing to about $+0.5\delta t$ toward the last of the 7839 coincidence candidates. Several of them are located away from this line, corresponding to bin pairs with accidental coincidences. The instantaneous time difference Δt of true coincidences increases only slowly with the binning index k, whereas the accidental coincidences can take arbitrary values. Thus, adjacent coincidence pairs with bin indices $k < k'$ with a difference $\Delta t_{j(k')} - \Delta t_{i(k)}$ in their instantaneous time difference exceeding a modulus of $(t_{j(k')} - t_{i(k)})/N$ are likely to contain at least one accidental coincidence. In a cleaning step, such pairs of adjacent candidates are simply removed. This step left only a small number of 348 coincidence candidates in the list, apparently without any accidentals (see figure 5(b)). A linear fit with a model $\Delta t = \Delta T' + \Delta u' t_i$ with data from the remaining pairs returns offset correction parameters $\Delta T' = 260.5 \pm 0.05$ ns and $\Delta u' = 4.270 \pm 0.002 \times 10^{-7}$. The error intervals from the fit appear overly optimistic, so we reconsider them, assuming a timing uncertainty of 1 ns in instantaneous measurements. We finally arrive at $\Delta T = 374\,593\,062 \pm 1$ ns and $\Delta u = -200\,789 \pm 1.4 \times 10^{-9}$.

These values are sufficient to start the tracking algorithm sketched in section 2. Figure 6 shows the evolution of the instantaneous time difference Δt, derived in a similar way as in figure 5(b), but with the data corrected by the previously obtained constants ΔT, Δu for modeling the reference clock difference. One can recognize the slow drift of the reference oscillators, suggesting a stability around 10^{-8} on a timescale of a second.

7. Conclusion

We have presented an algorithm to remotely identify correlated photon pairs generated in an SPDC process from a stream of detection times without the need for a dedicated hardware

channel, a very stable and accurate pair of reference clocks or a central clock source, which may expose the classical infrastructure of a QKD system to a risk of compromise. This greatly reduces the technical complexity of entanglement-based QKD systems, making this part of an effort to simplify hardware by using intrinsic information in the photon pairs and bringing it closer to applications.

Acknowledgments

This work is supported by the National Research Foundation and Ministry of Education, Singapore, and partly by a joint program of quantum information research between DSO and NUS.

Appendix. Iterative algorithm for finding time and frequency differences

An explicit algorithm for obtaining time and frequency differences ΔT and Δu from time sets $\{t_i\}$ and $\{t'_j\}$ with high precision comprises the following steps.

1. Choose the limits for the maximum expected frequency and time differences $\Delta u_{\max}$ and $\Delta T_{\max}$; the observed rates r_1, r_2 and an expected rate r_s can be used to check with equation (11) if this algorithm can be expected to be successful.
2. Choose an acquisition time interval T_a and a separation time interval T_s, e.g. $T_s = 10T_a$.
3. Choose the smallest discretization time δt that is compatible with a high chance of successfully identifying the correct peak in the cross correlation. Pair this with a suitable value of N for generating the arrays $\{a_j\}$ and $\{b_k\}$ according to equation (6).
4. Generate the cross correlation array $\{c_k\}$ via FFT as in section 3.
5. Find the index k of the maximal value in $\{c_k\}$ and estimate its statistical significance S according to equation (7).
6. If S is below a chosen significance limit S_{th}, halve the size of the array $\{c_k\}$ by adding entries pairwise, and go back to step 5; this doubles the effective time resolution $\delta t'$. Otherwise, continue.
7. Determine ΔT_1 from the peak position $k_{\max}$ and the effective time resolution $\delta t'$ of the last iteration of the previous step.
8. With the time resolution $\delta t'$ in step 6, generate discrete arrays $\{a_j\}$, $\{b_k\}$ and $\{c_k\}$ for the second sampling interval, and determine from there ΔT_2.
9. Determine Δu from ΔT_1, ΔT_2 and T_s from equation (10).
10. If $\delta t'$ in the last iteration is small enough to start the tracking as described in section 2, the algorithm is finished.
11. Generate a modified set of event times $\{\tilde{t}'_j\}$ according to $\tilde{t}' = (t' + \Delta T_1) \cdot (1 + \Delta u)$.
12. Choose the same N as in the last FFT, but reduce the time interval δt by less than the expected gain in accuracy given by $T_s/T_a/\sqrt{2}$; typically, this reduction factor would be 4 or 8 corresponding to 2 or 3 bits in accuracy gain.
13. Generate new $\{a_i\}$, $\{b_j\}$ and $\{c_k\}$ in the usual way from the original set $\{t_i\}$ and the modified set $\{\tilde{t}'_j\}$; from the peak position in the new $\{c_k\}$, determine the correction to ΔT_1. Usually, this adds 2 or 3 bits in accuracy to ΔT_1; proceed similarly for the correction to ΔT_2.
14. Continue with step 10.

References

[1] Scarani V *et al* 2009 *Rev. Mod. Phys.* to appear (arXiv:0802.4155v2 [quant-ph])
[2] Gisin N and Thew R 2007 *Nat. Photonics* **1** 165
[3] Dûsek M, Lütkenhaus N and Hendrych M 2006 *Prog. Opt.* **49** 381
[4] Bennett C and Brassard G 1984 *Proc. IEEE Int. Conf. on Computer Systems and Signal Processing (ICCSSP) (Bangalore, India)* p 175
[5] Ekert A 1991 *Phys. Rev. Lett.* **67** 661
[6] Bennett C H, Brassard G and Mermin N D 1992 *Phys. Rev. Lett.* **68** 557
[7] Acin A *et al* 2007 *Phys. Rev. Lett.* **98** 230501
[8] Kwiat P G *et al* 1995 *Phys. Rev. Lett.* **75** 4337
[9] Fedrizzi A, Herbst T, Poppe A, Jennewein T and Zeilinger A 2007 *Opt. Express* **15** 15377
[10] Trojek P and Weinfurter H 2008 *Appl. Phys. Lett.* **92** 211103
[11] Burnham D C and Weinberg D L 1970 *Phys. Rev. Lett.* **25** 84
[12] Poppe A *et al* 2004 *Opt. Express* **12** 3865
[13] Peng C Z *et al* 2005 *Phys. Rev. Lett.* **95** 030502
[14] Jennewein T, Simon C, Weihs G, Weinfurter H and Zeilinger A 2000 *Phys. Rev. Lett.* **84** 4729
[15] Marcikic I, Lamas-Linares A and Kurtsiefer C 2006 *Appl. Phys. Lett.* **89** 101122
[16] Ursin R *et al* 2007 *Nat. Phys.* **3** 481
[17] Ling A *et al* 2008 *Phys. Rev.* A **78** 020301
[18] Erven C, Couteau C, Laflamme R and Weihs G 2008 *Opt. Express* **16** 16840
[19] Holmes C A, Milburn G J and Walls D F 1989 *Phys. Rev.* A **39** 2493
[20] Mills D L 1991 *IEEE Trans. Commun.* **39** 1482
[21] Hough P 1959 *Proc. Int. Conf. on High Energy Accelerators and Instrumentation* ed L Kowarski (Geneva: CERN) pp 554–6 (also: Hough P V 1962 A method and means for recognizing complex patterns *US Patent Specification* 3069654)