Real-time phase tracking in single-photon interferometers

Vadim Makarov, Alexei Brylevski, and Dag R. Hjelme

A new technique for phase tracking in quantum cryptography systems is proposed that adjusts phase in an optimal way, using only as many photon counts as necessary. We derive an upper bound on the number of photons that need to be registered during phase adjustment to achieve a given phase accuracy. It turns out that most quantum cryptosystems can successfully track phase on a single-photon level, entirely with software, without any additional hardware components or extensive phase-stabilization measures. The technique is tested experimentally on a quantum cryptosystem. © 2004 Optical Society of America

OCIS codes: 030.5260, 040.5570, 060.5060, 120.5050, 270.1670.

1. Introduction

Quantum key distribution (QKD) systems are the new generation of cryptographic systems. They transmit a random key securely over an optical fiber (quantum channel). This random key is then used for encryption and decryption of confidential information, which then can be sent in encrypted form over any nonprotected communication channel. Over the past decade, quantum cryptosystems have been actively developed.

Most of the systems are based on fiber-optic interferometers. An inevitable problem for these interferometers is phase drift. The phase between the interferometers' arms has to be matched for transmission for interference results to be controllable. If no special measures are taken during assembly of the interferometer, the relative phase between the two arms can drift rather quickly (e.g. 0.6 rad/min as reported in Ref. 1 or 2 rad/min in our experiment described below).

Just how much inaccuracy is acceptable in phase matching? The probability of error is the ratio of error counts to the total number of counts. In an interferometric system, that would correspond to the lower part of the $\sin^2$ interference curve. Thus the contribution of phase mismatch $\Delta\varphi$ to the quantum bit-error rate (QBER) is

$$\mathrm{QBER}_{\mathrm{opt}\,\Delta\varphi} = \sin^2(\Delta\varphi/2),$$

which rises quadratically for small $\Delta\varphi$ (Fig. 1).

The key extraction algorithm can handle QBER up to a certain threshold value. This threshold value, according to some recent security analyses, is approximately 11%.[2–4] The larger the QBER, the bigger the part of the key that has to be discarded during key extraction, leaving us with a lower key exchange rate, which approaches zero as the QBER approaches 11%. A QBER value of 11% could be caused by a 38° phase mismatch if it were the only error source.

In real systems, other sources of error as well as $\mathrm{QBER}_{\mathrm{opt}\,\Delta\varphi}$ contribute to the total QBER. Some of these other sources of error (e.g., detector dark counts) are much harder to control than phase accuracy. We therefore want to keep $\mathrm{QBER}_{\mathrm{opt}\,\Delta\varphi}$ within ~1% (less if possible), to minimize its effect on the key exchange rate. This translates into a required phase accuracy of 10° or better.

2. Existing Solutions

There are three known ways to deal with phase drift:

(1) Use of a plug and play interferometer configuration (round-trip light propagation, autocompensating).

(2) Strict thermal and mechanical isolation (slows down phase drift).

(3) Periodic switching to bright light for active phase tracking.

(1) A plug and play system presents an elegant solution both for polarization fluctuations and for

V. Makarov (makarov@vad1.com) and D. R. Hjelme are with the Department of Electronics and Telecommunications, Norwegian University of Science and Technology (NTNU), NO-7491 Trondheim, Norway. A. Brylevski is with the Radiophysics Department, St. Petersburg State Polytechnical University, Politechnicheskaya Street 29, 195251 St. Petersburg, Russia.

Received 16 March 2004; revised manuscript received 16 March 2004; accepted 24 May 2004.

0003-6935/04/224385-08$15.00/0

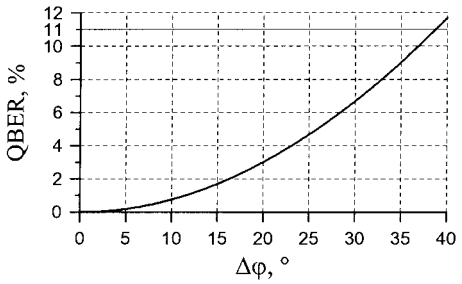

Fig. 1. QBER versus interferometer phase mismatch in the absence of other sources of error.

phase drift. In this approach, light pulses travel from Bob to Alice (Bob and Alice are common names for two communicating parties in cryptography), get reflected by a Faraday mirror, and then travel back to Bob: This automatically compensates for all polarization fluctuations in the transmission channel.[5,6] The two interfering pulses also follow exactly the same path in Alice's and Bob's interferometers, albeit in different directions: This automatically compensates for phase drift, eliminating the need for active adjustments.[7] A system of this type is easier to develop into a product than the other quantum cryptosystems and is the first one that is being deployed commercially.[8,9]

Unfortunately, the plug and play configuration has limitations, which stem from bidirectional light propagation:

- This configuration can only be used for QKD with faint laser pulses and with modulators in Alice's and Bob's setups. There are no plug and play configurations for entangled-pair-based schemes.
- The system is difficult to protect from external interrogation attacks (Trojan horse attacks), and it appears to be more vulnerable than others to implementation attacks.[10]
- It has a penalty factor of ~3 in the key generation rate compared with an equivalent non-plug-and-play configuration because, owing to Rayleigh backscattering from bright pulses, one cannot let light pulses propagate in opposite directions in the transmission channel at the same time. Pulses have to be transmitted in batches with pauses between them, and a fiber delay line employed in Alice's setup.[11]

(2) Passive measures such as thermal and mechanical isolation can, if done properly, keep phase sufficiently stable without adjustment for several hours. This is enough time for many laboratory experiments, in which initial adjustment or calibration is performed manually and is followed by a test run of limited duration. The phase, however, eventually drifts away. In a production system, automatic phase tracking would always be needed.

For example, the Quantum Optics group at the University of Geneva took careful measures to stabilize its interferometers such that experimental tests can be performed without continuous phase tracking. Those scientists keep interferometer arms reasonably short, i.e., a few tens of centimeters.[12,13] Their bulk-optics interferometer is built on a base made from material with a low thermal expansion coefficient and is thermoisolated as well.[14] Their fiber optics interferometers are packed into sand-filled copper tubes and are actively thermostabilized at a constant temperature by incorporation of a heater and a temperature sensor into the assembly.[15]

In another example, the EQUIS project aims at manufacturing Alice's and Bob's interferometers as integrated planar silica waveguide structures.[16] These devices are inherently more stable owing to their small size and monolithic construction. Each of them is thermostabilized by a thermoelectric heater–cooler, and the phase is reported to be "very stable".[17]

Thermostabilization can also be used to track phase if the heater–cooler is included in a feedback loop. It has the obvious disadvantage of a very long (of the order of hours) warm-up time[12]; moreover, it also takes a long time to stabilize the phase after the system suffers any mechanical or thermal impact.

(3) For rapid phase tracking, Marand and Townsend used two additional components to perform phase adjustment: a piezoelectric transducer with which to adjust the length of one of the arms of Alice's interferometer and an electrically switched attenuator.[1] The adjustment was performed by switching to low attenuation and scanning the phase by piezoelectric transducer until the photon count rate at one of Bob's output ports was minimized. The thermal phase drift rate reported by Marand and Townsend was ~0.6 rad/s.

Although it is possible to achieve slow phase drift rates by constructive measures, such measures make production more expensive and also can add bulk and weight to the equipment. It would be advantageous if standard fiber-optic assembly technology could be used, with standard splicing equipment, no severe restrictions on the length of fiber pigtails, and possibly with only light foam insulation around the assembled interferometer. Because such an interferometer exhibits a rather fast phase drift and makes it necessary to adjust phase every few seconds, as in Townsend's setup[1]; the phase adjustment itself should therefore be quick. There is, however, a problem of achieving desired phase accuracy in a short time: Existing quantum cryptosystems generate limited count rates at the detectors during normal operation (typically a few thousand counts per second), and statistical noise is significant.

For faint pulse systems that contain a laser and a strong attenuator, one can use an electrically switched attenuator to increase count rates temporarily during phase adjustment, as described in Ref. 1. This extra optical component, however, adds cost and lowers reliability (the system does need to employ some kind of adjustable attenuator to set the

mean photon number at the time of installation, but the attenuator need not be fast or even electrically controlled). It should also be possible to control the energy of the laser pulse electrically (by changing its brightness, duration, or both), but we are not aware of any tests that have been made of this technique in quantum cryptosystems.

Most important, for systems based on single-photon and photon-pair sources (e.g., parametric downconversion sources), increasing light output of the source can be impractical or impossible.

We therefore decided to find a technique that does not require any extra components and performs phase adjustment entirely with software, at the single-photon level, utilizing only as many detector counts as are necessary to achieve the required phase accuracy.

The research that comes closest to this idea is an experiment that was performed at the Los Alamos National Laboratory. It was suggested that the feedback signal for phase tracking be derived from key data ("from the key error rate and key bias"[18]). However, no further details have been published, to our knowledge. That interferometer contains air gaps driven by piezoelectric transducers to control the phase on both Alice's and Bob's sides. The published experimental results hint at constructive isolation as well: phase appears to be stable without adjustment over time span of 10 min, and the interferometer boxes are quite bulky.

3. Phase-Tracking Algorithm

The QKD setup that we consider consists of a Mach–Zehnder interferometer with a phase modulator in each arm. The phase modulator in one arm resides on Alice's side, and the phase modulator in the other arm resides on Bob's side. Single-photon detector(s) reside on Bob's side. For more details we refer the reader to Section 4 below and to Refs. 1 and 19.

For the whole duration of adjustment, Alice sets her phase modulator to zero (0 V) and transmits photons as usual. Only Bob's phase modulator is used.

The software phase-tracking algorithm that we devised consists of two stages: stage 1 for rough phase adjustment and stage 2 for fine phase compensation.

A. Stage 1: Rough Phase Compensation

In stage 1, Bob scans the whole phase range (0°–360°) in a small number of steps, using his modulator, and records the number of detector counts collected at each step by 0 and 1 photon detectors (or in 0 and 1 detector time slots if only one photon detector is used in the system). He then notes the phase settings of his modulator at which the smallest number of counts occurred in the 0 detector time slot and in the 1 detector time slot. The value of the phase setting for the 1 time slot can be either less or greater than the value of the phase setting for the 0 time slot, depending on the position of the interference curves in the scanning range. In the former case, we add 180° to the value of phase setting for the 1 time slot; in the latter case, we subtract 180° from the value of phase setting for the 1 time slot. After this, we calculate an average of the values for the 0 and the 1 time slots, which improves accuracy. This average is assumed to be the roughly determined phase compensation, φ_0.

This scan allows Bob to determine quickly the positions of minima of interference curves with an accuracy of 20°–30°. Further improvement of precision requires a different method, because the $\sin^2$-shaped interference curves both are flat and have the highest relative statistical fluctuations near their minima. To get the best accuracy in a given counting time, we propose to count photons at the points on the interference curves where the photons have the maximum slope-to-statistical-deviation ratio. To the first approximation, these points are $\varphi_0 + 90°$ and $\varphi_0 - 90°$. We do this counting in stage 2.

The purpose of stage 1 is to provide quickly a rough estimate of these points. However, stage 1 need not be repeated on subsequent runs of phase adjustment if it is known that the phase has not deviated much. This lack of deviation can be inferred from a successful key exchange immediately before the phase adjustment or can be guaranteed by the time since the last run combined with the fastest estimated drift rate.

B. Stage 2: Fine Phase Compensation

In stage 2, Bob switches his modulator from $\varphi_0 + 90°$ to $\varphi_0 - 90°$ and back in a symmetric square-wave pattern and records the number of photon counts at each phase setting. He obtains four count values:

N_{0+}, the number of photons detected at the $\varphi_0 + 90°$ phase setting in the 0 time slot;
N_{0-}, the number of photons detected at the $\varphi_0 - 90°$ phase setting in the 0 time slot;
N_{1+}, the number of photons detected at the $\varphi_0 + 90°$ phase setting in the 1 time slot;
N_{1-}, the number of photons detected at the $\varphi_0 - 90°$ phase setting in the 1 time slot.

In Fig. 2, Function 0 is our assumption of the position of interference curve $N(\varphi)$ after the first stage of phase adjustment has been performed, with the minimum at φ_0. Function 1 is a more-accurate position of interference curve $N(\varphi)$, with the minimum at φ_1, which is unknown to us at this point:

$$\text{Function 0} \qquad N = (N_{\max} - N_{\min})\sin^2\left(\frac{\varphi - \varphi_0}{2}\right) + N_{\min}$$

$$\text{Function 1} \qquad N = (N_{\max} - N_{\min})\sin^2\left[\frac{\varphi - (\varphi_0 + \delta)}{2}\right] + N_{\min}, \qquad \delta = \varphi_1 - \varphi_0.$$

Using the equations above, one can derive correction δ as a function of $N_{0+}, N_{0-}, N_{1+}, N_{1-}, N_{\min}$, and $N_{\max}$ (for a full derivation, see Ref. 20). $N_{\min}$ and $N_{\max}$

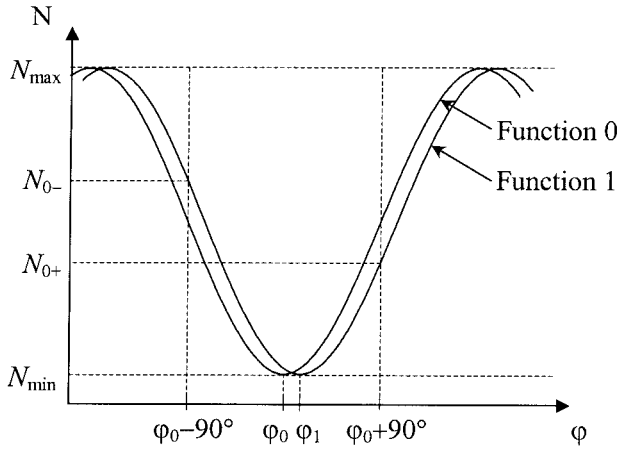

Fig. 2. Illustration of phase adjustment at stage 2. Only the interference curve for the 0 time slot is shown.

can actually be different for 0 and 1 time slots, so we split them into $N_{\min 0}$, $N_{\min 1}$, $N_{\max 0}$, and $N_{\max 1}$. The correction becomes

$$\delta = \frac{1}{4}\left[\arccos\left(2\,\frac{N_{\min 0}-N_{0+}}{N_{\max 0}-N_{\min 0}}+1\right) - \arccos\left(2\,\frac{N_{\min 0}-N_{0-}}{N_{\max 0}-N_{\min 0}}+1\right) + \arccos\left(2\,\frac{N_{\min 1}-N_{1-}}{N_{\max 1}-N_{\min 1}}+1\right) - \arccos\left(2\,\frac{N_{\min 1}-N_{1+}}{N_{\max 1}-N_{\min 1}}+1\right)\right]. \quad (1)$$

In the experiment we assumed that $N_{\min 0} = N_{\min 1} = 0$, $N_{\max 0} = N_{0+} + N_{0-}$, and $N_{\max 1} = N_{1+} + N_{1-}$. $N_{\min 0}$ and $N_{\min 1}$ are in practice nonzero because of imperfect fringe visibility and detector dark counts. They can be estimated more precisely, should that be necessary.

The resultant correction δ is added to φ_0 to yield the more-accurate value of phase compensation, φ_1. The voltage corresponding to φ_1 is applied as an offset voltage to Bob's phase modulator during the key transmission session that follows phase adjustment.

There will be some random error in φ_1, owing to statistical fluctuations in the number of counts N_{0+}, N_{0-}, N_{1+}, and N_{1-}. We can calculate how many counts need to be collected to achieve a given phase accuracy with a certain probability.

The interference curve is given by

$$N = (N_{\max} - N_{\min})\sin^2\left(\frac{\varphi-\varphi_1}{2}\right) + N_{\min},$$

such that

$$\frac{dN}{d\varphi} = \frac{1}{2}(N_{\max} - N_{\min})\sin(\varphi-\varphi_1).$$

Thus at our $\pm 90°$ counting points the slope of the interference curve is approximately

$$\frac{\Delta N}{\Delta\varphi} = \frac{1}{2}(N_{\max} - N_{\min}). \quad (2)$$

N obeys a Poisson distribution, which approaches a Gaussian distribution for the relatively large mean number of counts involved. Assuming that $N_{\min} = 0$ and $N = N_{\max}/2$, statistical error level ΔN follows as

$$\Delta N = k\sigma = k\sqrt{N_{\max}/2}, \quad (3)$$

where σ is the standard deviation and k is the number of standard deviations that corresponds to a given probability that the actual number of counts will fall within $(N - \Delta N, N + \Delta N)$. Combining Eqs. (2) and (3), we obtain

$$N_{\max} = 2(k^2/\Delta\varphi^2).$$

Assuming that $N_{\max} = N_{0+} + N_{0-}$, we have

$$N_{0+} + N_{0-} = 2(k^2/\Delta\varphi^2). \quad (4)$$

This is the number of counts needed to achieve a phase error of $\Delta\varphi$ or less, where the probability of not exceeding this phase error is set by the number of standard deviations k. Actually, we are collecting counts in both detection windows, not just in one, and obtain phase correction by averaging over all four count values according to Eq. (1). Averaging works such that the same right-hand side of Eq. (4) would then estimate the total number of counts:

$$N_{0+} + N_{0-} + N_{1+} + N_{1-} = 2(k^2/\Delta\varphi^2). \quad (5)$$

For example, to achieve our goal of 10° or better accuracy in, say, 95% of the phase-adjustment attempts ($k = 2$), it would suffice to register approximately

$$N_{0+} + N_{0-} + N_{1+} + N_{1-} = 2\,\frac{2^2}{[(10°/180°)\pi]^2} = 262 \text{ counts} \quad (6)$$

in stage 2 of the phase adjustment. We have also determined empirically that stage 1 requires fewer counts than stage 2 (this is illustrated below).

Equation (5) provides an upper-bound estimate for the number of counts required. Whether a more count-efficient phase-adjustment algorithm exists remains an open question.

Using the estimate given in Eq. (6), one could check whether a quantum cryptosystem can function with software-only phase tracking or whether it needs one of the additional measures reviewed in Section 2. To do the check we need to know the fastest phase drift rate in the interferometer and the lowest photon-counting rate possible in the specified range of operating conditions in which the system will be used. The operating conditions that affect the phase drift rate will be the environment (temperature, humidity, vibration, etc.) in which the end equipment is

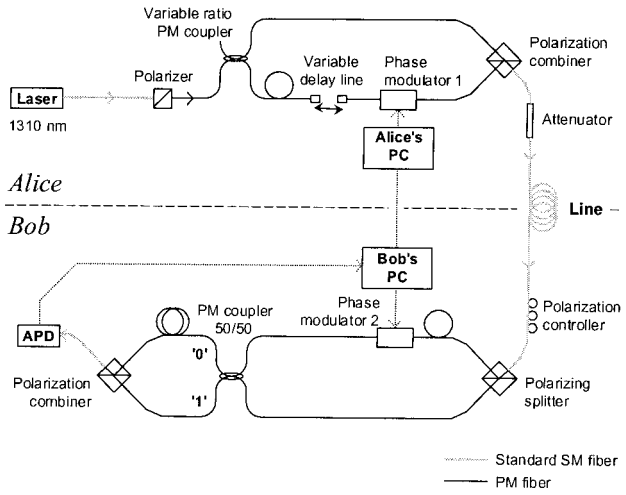

Fig. 3. QKD setup: SM, single-mode; other abbreviations defined in text.

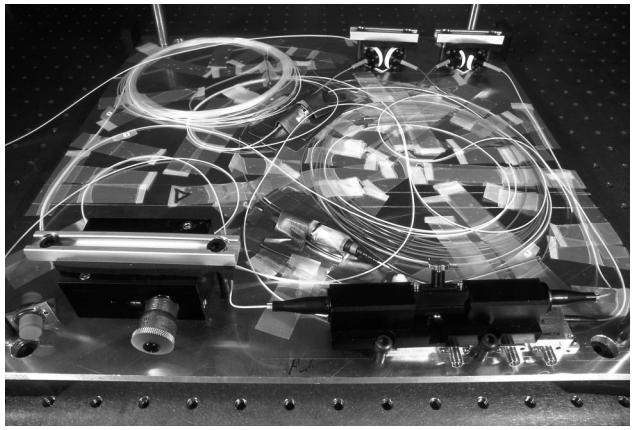

Fig. 4. Bob's interferometer. All components are mounted on a 400 mm × 400 mm × 6 mm aluminum plate, and their fiber pigtails are affixed to the plate surface with pieces of adhesive tape. Everything is covered by custom-cut pieces of foam insulation (not shown in the photo) and mounted inside a box. Alice's interferometer is similar.

installed. The operating condition that determines the photon-counting rate will be primarily the line attenuation (currently limited by the dark-count rate of the detectors). Knowing these two rates, one can check how far the phase can drift during the time required to collect ~200 counts. If the phase drifts away by significantly less than 10° during that time, it can be tracked easily by use only of the periodic phase adjustment described in this paper; only a fraction of the channel time would be spent on phase tracking, leaving most of the channel capacity to QKD. If, however, the phase drifts away by more than 10°, additional hardware measures are needed to slow down phase drift, speed up phase adjustment, or both. This is just a rule of thumb. If the actual drift rate falls close to this figure, the necessity for hardware measures would depend on the exact design of the system, on trade-offs, and on reliability margins; discussing this gray zone is beyond the scope of this paper.

4. Experiment

We tested the phase-adjustment algorithm on our QKD setup.

A. Experimental Setup

The QKD setup uses a time- and polarization-multiplexed Mach–Zehnder interferometer (general scheme proposed by Townsend *et al*. in Ref. 19) and the BB84 protocol.[21] The optical setup is shown schematically Fig. 3.

Light pulses that are 100 ps wide are emitted by a 1310-nm semiconductor laser at a 10 MHz rate. The arms of the interferometer are made from polarization-maintaining (PM) fiber (Fujikura PANDA fiber); everything is aligned such that light propagates in the slow-axis mode of PM fiber. One arm of the interferometer in Alice's setup is ~2 m long, whereas the other arm is ~6 m long; the arms in Bob's setup are also ~6 and ~2 m long. The phase modulators are the lithium niobate planar-waveguide type (Alenia Marconi-made at Alice's side and Uniphase-made at Bob's side); they pass only one polarization. The phase modulators have a half-wave voltage of several volts, and each is controlled by a high-speed digital-to-analog converter card. The pulses from the two arms of the interferometer have orthogonal polarization in the line and are also separated in time. A polarization controller restores the polarization state of the pulses after the line such that the pulses split properly into two arms. Imperfect adjustment of this polarization controller and small polarization fluctuations in the line should affect neither phase tracking nor QKD, because if a part of the pulse is split into the wrong arm the wrongly split part arrives at the detector outside its detection windows, and because phase tracking is not sensitive to fluctuations in absolute light level.

Alice's and Bob's setups are mounted onto an aluminum plate (Fig. 4) and covered with thermoisolation. As it turned out, this kind of construction exhibits a phase drift rate of as much as 2 rad/min when it is left at rest in normal indoor conditions (in an optical lab).

The avalanche photodiode (APD) is gated at 20 MHz. This relatively high gating frequency is made possible by the use of an afterpulse blocking technique.[22] Data from the APD are buffered in a 4-Mbit first-in–first-out memory before they are read into Bob's PC. We use a Soviet-made Ge APD (standard part number FD312L, developed by NPO Orion), placed inside a liquid-nitrogen tank. The best APD sample that we have has a 5×10^{-5} dark-count probability at 16% quantum efficiency. Given a 4.2-dB measured loss in Bob's optical setup, 0.5-dB/km losses in fiber at 1310 nm, an acceptable contribution of detector dark counts to the bit error rate $\mathrm{QBER}_{\mathrm{det}}$ of, say, 4%, and mean photon number per pulse at Alice's output of $\mu = 0.2$, the APD that we have would allow for an ~20-km-long QKD link.

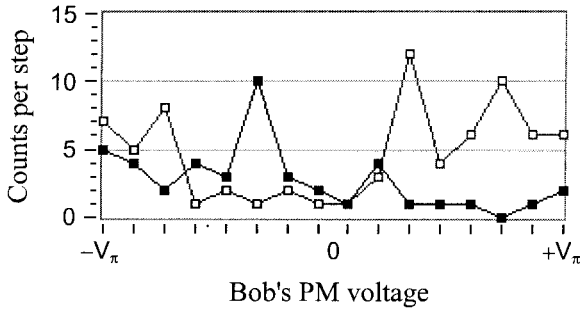

Fig. 5. Interference curves for the 0 (filled squares) and 1 (open squares) time slots, plotted from data measured in a single run of stage 1 phase adjustment. The 2π phase range was scanned in 16 steps, and on average 150 counts were collected in stage 1.

With the APD that we have, the photon-counting rate in the system at the longest possible link length would be no fewer than 5000 counts/s (at which rate $QBER_{det}$ would closely approach 11%). The 200 counts required for a phase adjustment would be accumulated in at most 40 ms. Given the fastest phase drift rate measured, a drift of as much as 0.08° can occur in this time. Thus, according to the criterion given in the end of Section 3, the system is well suited to software-only phase tracking. $QBER_{opt\ \Delta\varphi}$ and time spent on phase adjustment would not reduce the key generation rate much.

At the time of the phase-tracking experiment, our system was not ready to demonstrate QKD (most notably because of poor fringe visibility of ~0.8, which has since been improved to 0.92, and because of Alice's faulty digital-to-analog converter card). However, this has not affected the phase-tracking algorithm, which we have successfully tested.

B. Results for Phase Tracking

In our tests, phase adjustment is performed every 3 s, which corresponds to a phase drift of as much as 6° between adjustments. The data are captured in the first-in–first-out memory in less than 40 ms, but processing them actually takes much longer than that, because readout from the memory and other operations are slow owing to inefficient software (mostly written in LabVIEW for the purposes of the experiment). To reduce readout time, we increased μ to 0.37, and we use no transmission line (i.e., Alice is connected directly to Bob). This should not affect test results for phase tracking, however.

In the first test run we performed both stage 1 and stage 2 phase adjustment each time, using rough phase compensation φ_0 from stage 1 as a starting point for stage 2. Figure 5 shows typical data collected in stage 1. Statistical noise at such a low average number of counts yields wildly varying shapes, which are hardly recognizable as interference curves at first glance. If we collected many more counts in stage 1, we would indeed see nice sine- and cosine-shaped curves. However, even these noisy data allow reliable determination of φ_0 with an accuracy of 20°–30°, as Fig. 6, top, illustrates. φ_0 is then used as input to stage 2. Results of stage 2 are shown in the lower part of Fig. 6, which is less noisy and shows that stage 2 works well with these input data.

In fact, stage 1 is not important, and we treat it here in such detail only to study the whole problem better. In a properly working system, one can al-

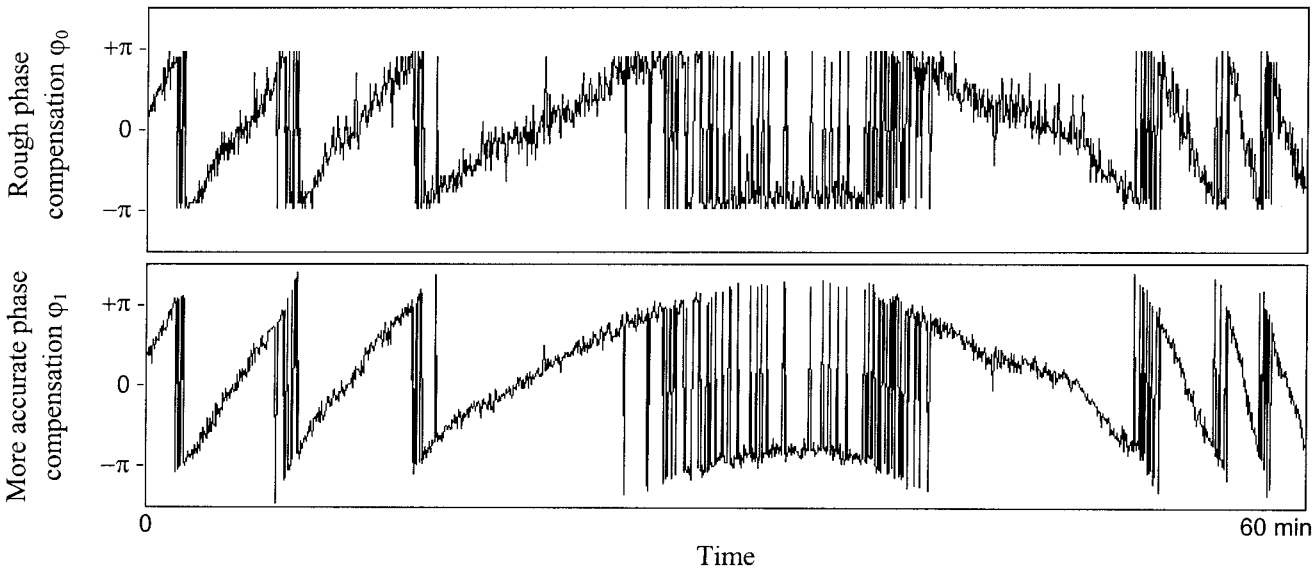

Fig. 6. Voltage in Bob's phase modulator, scaled to the equivalent phase shift. A 1-h fragment of phase tracking data from a test run with both stage 1 and stage 2 phase adjustment performed each time. Phase adjustment is run every 3 s; the average number of counts collected in stage 1 is 150 and in stage 2 is 230. Vertical hops in the figures do not represent any phase discontinuity (the phase is cyclic over 2π) but do represent jumps in phase modulator voltage, because we had to stay within the voltage range of our phase modulators limited to just over $\pm V_\pi$. If we neglected jumps in phase modulator voltage and printed cylindrically shaped graphs for phase, there would be no hops on them.

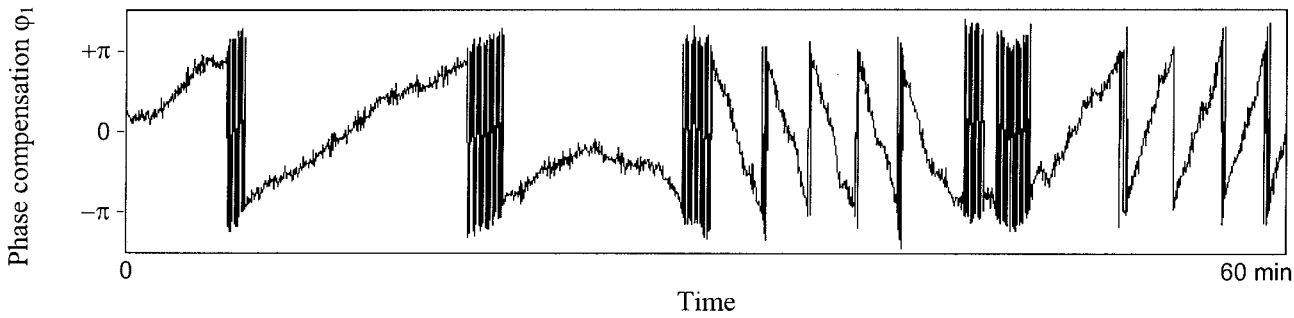

Fig. 7. Voltage of Bob's phase modulator, scaled to the equivalent phase shift. A 1-h fragment of phase tracking data from a test run with only stage 2 of the phase adjustment performed each time. Phase compensation from previous phase adjustment is used as input to stage 2. Phase adjustment is run every 3 s, and the average number of counts is 230 for each adjustment.

ways take the phase compensation from the previous phase adjustment and use it as input to stage 2. This is what we did on the second test run, illustrated in Fig. 7.

Judging from the width of the noise trace in Fig. 7, our goal of 10° or better phase accuracy most of the time is achieved. It is not possible to assess statistical fluctuations quantitatively, because in this experiment we do not know the underlying phase drift with better accuracy. However, the smoother parts of the curve suggest that the level of statistical fluctuations is close to what is expected in our phase-tracking algorithm. To quantify the error level accurately we would need to run a control phase measurement in parallel, which our setup is not equipped to do. It would be also possible to confirm the performance of phase tracking by the results of QKD if $\mathrm{QBER}_{\mathrm{opt}\,\Delta\varphi}$ made a major contribution to the total QBER (which is not the case with our setup: The contribution that is due to poor fringe visibility would dominate, masking $\mathrm{QBER}_{\mathrm{opt}\,\Delta\varphi}$).

Looking at the figures, one can easily note that phase drift in our interferometer is not entirely random but occurs mostly at a slowly changing rate. This may allow us to further reduce the number of counts required for phase adjustment, i.e., to do better than in Eq. (5), because we could partly predict the phase by extrapolating recent tracking data.

5. Conclusions

The phase-adjustment technique described in this paper tracks phase drift in interferometers at the low light levels that are typical for single-photon applications. This gives the designer of a quantum cryptography system new degrees of freedom. Using these results, one can accurately estimate requirements for successful phase tracking. In most cases it is possible to construct interferometers without heavy thermoisolation and without additional components such as a fast electrically controlled variable attenuator, at the cost of performing some programming. In effect, expensive hardware measures are replaced by software.

We hope that this study will facilitate the development of advanced and more-secure types of quantum cryptosystems into commercial products.

This study was supported by Norwegian Research Council project 119376/431. The authors thank Astrid Dyrseth for help with LabVIEW programming and Lars Johnsen and Noralf Ryen for designing electronics and bits of metal hardware.

Visit our project Web site at http://www.vad1.com/qcr/.

References and Notes

1. C. Marand and P. Townsend, "Quantum key distribution over distances as long as 30 km," Opt. Lett. **20,** 1695–1697 (1995).
2. The threshold value of QBER is still being discussed. Most recent strict security analyses, however, put it at 11%. For a review, see for example Refs. 3 and 4 and references therein.
3. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," Rev. Mod. Phys. **74,** 145–195 (2002).
4. M. Bourenanne, A. Karlsson, G. Bjork, N. Gisin, and N. J. Cerf, "Quantum key distribution using multilevel encoding: security analysis," J. Phys. A Math. Gen. **35,** 10,065–10,076 (2002).
5. M. Martinelli, "A universal compensator for polarization changes induced by birefringence on a retracting beam," Opt. Commun. **72,** 341–344 (1989).
6. M. Martinelli, "Time reversal for the polarization state in optical systems," J. Mod. Opt. **39,** 451–455 (1992).
7. H. Zbinden, J. D. Gautier, N. Gisin, B. Huttner, A. Muller, and W. Tittel, "Interferometry with Faraday mirrors for quantum cryptography," Electron. Lett. **33,** 586–588 (1997).
8. D. Stucki, N. Gisin, O. Guinnard, G. Ribordy, and H. Zbinden, "Quantum key distribution over 67 km with a plug & play system," New J. Phys. **4,** 41.1–41.8 (2002).
9. As of March 2004, one could place an order for a complete quantum cryptosystem with a plug and play type of optical scheme with two companies: id Quantique (Geneva, Switzerland, http://www.idquantique.com/) and MagiQ Technologies (Boston, Mass., http://www.magiqtech.com/).
10. A. Vakhitov, V. Makarov, and D. R. Hjelme, "Large pulse attack as a method of conventional optical eavesdropping in quantum cryptography," J. Mod. Opt. **48,** 2023–2038 (2001).
11. G. Ribordy, J.-D. Gautier, N. Gisin, O. Guinnard, and H. Zbinden, "Automated plug & play quantum key distribution," Electron. Lett. **34,** 2116–2117 (1998).
12. W. Tittel, J. Brendel, H. Zbinden, and N. Gisin, "Quantum cryptography using entangled photons in energy-time Bell states," Phys. Rev. Lett. **84,** 4737–4740 (2000).
13. W. Tittel, J. Brendel, N. Gisin, and H. Zbinden, "Long-distance

Bell-type tests using energy-time entangled photons," Phys. Rev. A **59,** 4150–4163 (1999).
14. G. Ribordy, J. Brendel, J.-D. Gautier, N. Gisin, and H. Zbinden, "Long-distance entanglement-based quantum key distribution," Phys. Rev. A **63,** 012309 (2001).
15. Hugo Zbinden, Group of Applied Physics—Optique, Université de Genève, Rue de l'École-de-Médecine 20, CH-1211 Geneva 4, Switzerland (personal communication, 2001).
16. S. Pellegrini, "EQUIS project," http://www.phy.hw.ac.uk/resrev/EQUIS/; see p. WP4, "Integrated Mach–Zehnder/Michelson interferometer."
17. G. Bonfrate, "Integrated optics for practical quantum cryptography systems," presented at the Second Quantum Information Processing and Communications Workshop, Turin, Italy, 28–31 October 2001.
18. R. Hughes, G. Morgan, and C. Peterson, "Practical quantum key distribution over a 48-km optical fiber network," J. Mod. Opt. **47,** 533–547 (2000).
19. P. Townsend, J. Rarity, and P. Tapster, "Enhanced single photon fringe visibility in a 10 km-long prototype quantum cryptography channel," Electron. Letters **29,** 1291–1293 (1993).
20. A. Brylevski, "Quantum key distribution: real-time compensation of interferometer phase drift," M.S. thesis [written at the Department of Physical Electronics, Norwegian University of Science and Technology (NTNU) and defended at the Department of Radiophysics, St. Petersburg State Technical University, St. Petersburg, Russia, 2002], http://www.vad1.com/qcr/alexey/.
21. C. H. Bennett and G. Brassard, "Quantum cryptography: public key distribution and coin tossing," in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing* (Institute of Electrical and Electronics Engineers, New York, 1984), pp. 175–179.
22. K. Vylegjanine, "High-speed single photon detector for quantum cryptosystems," M.S. thesis [written at the Department of Physical Electronics, Norwegian University of Science and Technology (NTNU) and defended at the Department of Radiophysics, St. Petersburg State Technical University, St. Petersburg, Russia, 2000], http://www.vad1.com/qcr/kirill/.

On choice of points for stage 2 of phase tracking algorithm

In the paper we wrote: "To get the best accuracy in a given counting time, we propose to count photons at the points on the interference curves where they have the maximum slope-to-statistical-deviation ratio. To the first approximation, these points are φ_0+90° and φ_0–90°." Let's show that this assumption is correct.

The slope of the interference curves for the "0" and "1" detectors (assuming symmetrical curves for both detectors) depends on phase φ as

$$S_0 = \frac{d}{d\varphi}\left[(1-2e)\sin^2(\varphi/2)+e\right] = S_1 = \frac{d}{d\varphi}\left[(1-2e)\cos^2(\varphi/2)+e\right]$$
$$= \frac{(1-2e)\sin\varphi}{2} \propto (1-2e)\sin\varphi, \tag{7}$$

where e is a parameter that depends on the fringe visibility and detector dark count level and shows how far the lowest ponts on the curve are from zero. The parameter e is chosen to be equivalent to QBER in the case when imperfect fringe visibility and detector dark counts are the only contributions to QBER (which is nearly always so in the absence of eavesdropping). Let's call e the base level. A typical QKD setup will work at the values of e ranging from less than two percent (at short distances and with good optical alignment) to around 10% at the distance limit.

The statistical deviations (in approximation of Gaussian distribution) depend on phase as

$$D_0 = \sqrt{\langle N_0(\varphi)\rangle} \propto \sqrt{(1-2e)\sin^2(\varphi/2)+e}$$
$$D_1 = \sqrt{\langle N_1(\varphi)\rangle} \propto \sqrt{(1-2e)\cos^2(\varphi/2)+e}. \tag{8}$$

It can be shown that, if we have two channels carrying the same useful signal with amplitudes S_0 and S_1 mixed with statistically independent Gaussian noise with root-mean-square amplitudes D_0 and D_1 respectively, these two channels can be added together with weights m/S_0 and $(1-m)/S_1$, where

$$m = \frac{1}{\left(\frac{D_0}{S_0}\frac{S_1}{D_1}\right)^2 + 1}, \tag{9}$$

in order to obtain a single channel with the best signal to noise ratio. Our two interference curves present the same situation: they have the slope, which directly translates to the amplitude of the useful error signal, and different statistical deviations (i.e. noise). The *effective* slope-to-statistical-deviation ratio after summing as described above is

$$\frac{S_{\text{eff}}}{D} \propto \frac{S_0}{D_0}\frac{S_1}{D_1}\sqrt{\left(\frac{D_0}{S_0}\right)^2+\left(\frac{D_1}{S_1}\right)^2} = \frac{(1-2e)\sin\varphi}{\sqrt{\frac{(1-2e)^2}{4}\sin^2\varphi + e(1-e)}}. \tag{10}$$

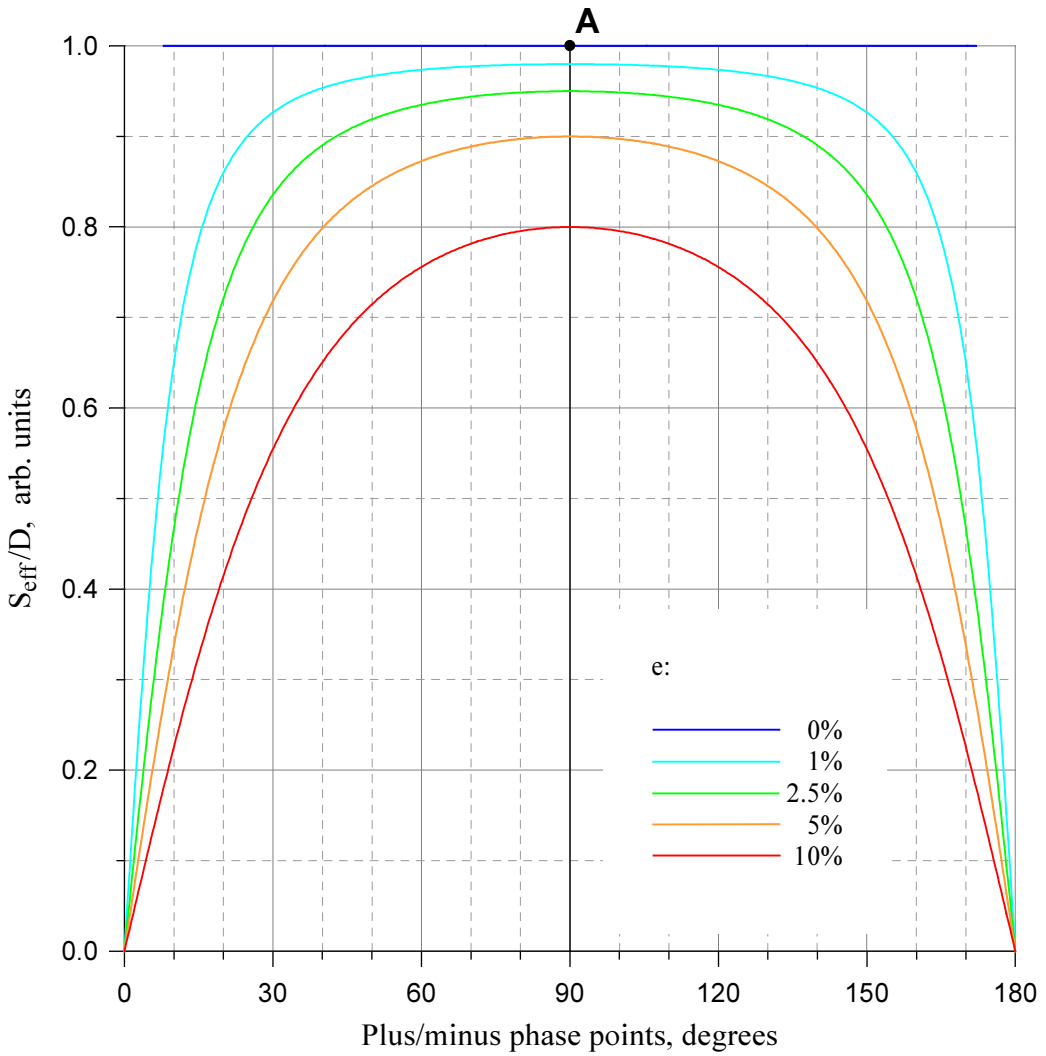

Fig. 8. Effective slope to statistical deviation ratio S_{eff}/D as a function of φ (Eq. 10) plotted for several values of base level *e* typical for quantum cryptography setups (*e*=0.01 (1%) to *e*=0.1 (10%)) as well as for *e*=0. Note that the Gaussian approximation assumed in the derivation may not hold near 0° and 180° for the *e*=0 curve.
A: point used for all derivations in the above paper.

Let's plot S_{eff}/D as a function of φ for several values of the base level *e* (Fig. 8). We see that for non-zero values of *e*, the best S_{eff}/D is actually achieved at the chosen ±90° points, so the assumption in the paper is correct.*

* Only S_{eff}/D peaks at ±90°. S_0/D_0 and S_1/D_1, i.e., the slope-to-statistical-deviation ratios for individual interference curves (not plotted), peak at phase points less than ±90° off the minimum of each interference curve; however, their values are always lower than the peak value of S_{eff}/D.

Effect of non-zero QBER on required number of counts

In the paper, the assumption of $N_{\min}=0$ was made when deriving Eqs. (3)–(6). In fact, $N_{\min}>0$, i.e. $e=\mathrm{QBER}>0$, leads to gentler slope of the interference curves, so more counts need to be collected in stage 2 to achieve the same phase accuracy. Figure 8 can be used to estimate the difference. The point marked **A** corresponds to the S/D ratio used in the paper. The actual S/D ratio depends on e and is in practice lower (see where the curves cross the 90° vertical line). To obtain the actual number of counts required, the right hand side of Eqs. (5) and (6) should be multiplied by the factor of

$$\left(\frac{\text{S/D for } e=0}{\text{S/D for a given } e>0}\right)^2=\left(\frac{1}{1-2\cdot\mathrm{QBER}}\right)^2. \tag{11}$$

This factor can be as large as 1.56 for systems working around their distance limit (i.e., at QBER=10%). This correction is sufficiently large and must be taken into account.

Using data discarded during sifting for phase tracking

One may notice that the key bits discarded by Alice and Bob on the sifting stage (i.e. those bits detected by Bob in a basis incompatible with Alice) could be used for phase tracking. Indeed, these Bob's detections are at the ±90° points from the extrema of the interference curves. Perhaps this is what Hughes and coworkers have meant in Ref. 18. However, this would require Alice to divulge her bit values for these bits to Bob (and to Eve) over the public channel. One should be very careful to see if such a disclosure fits well with the general security proof. This remains an open question. If it can't be shown that the security proof holds in such a case, then the phase adjustment must be performed separately from key generation.