Path-length control in a interferometric QKD link

Brig B. Elliott, Oleksiy Pikalo, John Schlafer, Greg Troxel
BBN Technologies, 10 Moulton St, Cambridge, MA 02138 USA

ABSTRACT

We describe a phase-encoded quantum key distribution system that uses continuous control of receiver - interferometer path length to maintain alignment with the transmitter. In this fiber-based system, a small number of training frames are sent over the quantum channel that allow the receiver to compensate for drift in the transmitter and receiver interferometers due to slow changes in temperature. The system is self-starting after disruption and can maintain a quantum bit error rate of less than 7% for phase drift rates of 0.5 deg/sec. The control system design is described and measured system data is compared with simulations.

Keywords: Quantum cryptography, quantum key distribution, path-length control

1. INTRODUCTION

A Quantum Key Distribution (QKD) link, built as a part of the DARPA Quantum Network program, employs the BB84 protocol in a weak-coherent system that encodes qubit values in the phase of a photon. This scheme was first proposed in 1992 letter by Bennett and has been implemented several times by various research teams.[1, 2] Such systems employ interferometers that must be configured to compensate for changes induced by environmental factors such as temperature and fiber stress level.

Figure 1 highlights the major components of our weak-coherent link. The transmitter (Alice) sends single photons by means of a highly attenuated laser pulse at 1550 nm. Each photon passes through a Mach-Zehnder interferometer, one arm of which is randomly phase modulated to one of four phase settings, thus encoding both a bit value and a basis, $\Phi_{Va} + \Phi_{Ba}$, in the photon's phase. Alice's interferometer is unbalanced and, when illuminated with 0.5 ns pulses, two time-spaced wave packets emerge at Alice's output. The receiver (Bob) also contains a similar unbalanced interferometer, with one arm randomly modulated to one of two basis phases Φ_{Bb} used by Alice. Ideally, the differential delay in both Bob's and Alice's interferometer is identical to within a few wavelengths and stable to within a fraction of the QKD photon's wavelength. When the two pulses from Alice enter Bob's interferometer they are split into two sets of two that combine at the output such that the leading pulse of one set overlaps the trailing pulse of the other set. Interference in the overlapping wave functions creates a central pulse whose probability of striking either detector is dependent on the relative phases of the two waves, set by the total phase shift introduced at Alice and Bob, $\Phi_0 = \Phi_{Va} + \Phi_{Ba} - \Phi_{Bb}$. When the total phase shift is $\Phi_0 = 0$, for example, the intensity is maximum at the detector $D^{(0)}$ and minimum at the detector $D^{(1)}$. A single photon is more likely to strike detector $D^{(0)}$, representing a received value of zero. When the total phase shift is $\Phi_0 = \pi$, the reverse is true: the photon is more likely to strike $D^{(1)}$, which represents a received value of one.

For the link to operate properly the differential delay caused by the short and long arms of each interferometer should be the same and remain stable to within a fraction of the QKD wavelength. This state is difficult to maintain over long periods of time, since the interferometers are in different locations and subject to different temperature, pressure and stress conditions. Environmentally-induced changes in differential delay contribute to the applied phase shift, Φ_0, and result in a higher quantum bit error rate (QBER) and disruption of the operation of the quantum link. The total phase shift is therefore $\Phi = \Phi_0 + \Delta\Phi$, where $\Delta\Phi$ is an extraneous

Further author information: (Send correspondence to B.B.E.)
B.B.E.: E-mail: celliott@bbn.com, Telephone: 1 617 873 2615
O.P.: E-mail: opikalo@bbn.com
J.S.: E-mail: jschlafer@bbn.com
G.T.: E-mail: gtroxel@bbn.com

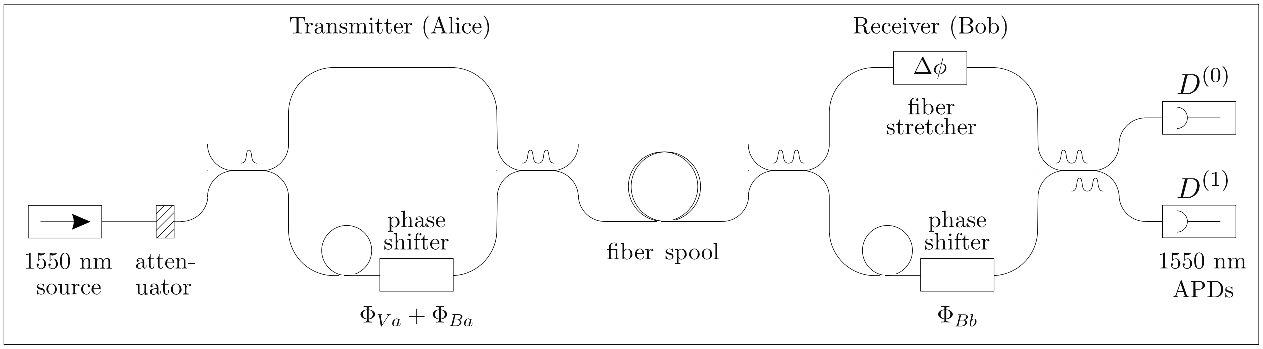

Figure 1. Unbalanced double Mach-Zehnder interferometer setup of the weak-coherent QKD link. The spacial relationship of optical pulses entering and exiting the interferometers is illustrated. $D^{(0)}$ and $D^{(1)}$ are avalanche photodiode (APD) detectors.

phase shift. A graph of the modeled[3] and measured QBER vs. $\Delta\Phi$ is presented in Figure 2. The parameters of the system are as follows: pulse rate of 1 Mb/sec; photon mean number $\mu = 0.1$ photon; 10 dB fiber and receiver loss; detector efficiencies of 0.147 for $D^{(0)}$ and 0.152 for $D^{(1)}$; dark-count probabilities of 12×10^{-6} and 37×10^{-6}; 96% interferometer fringe visibility.

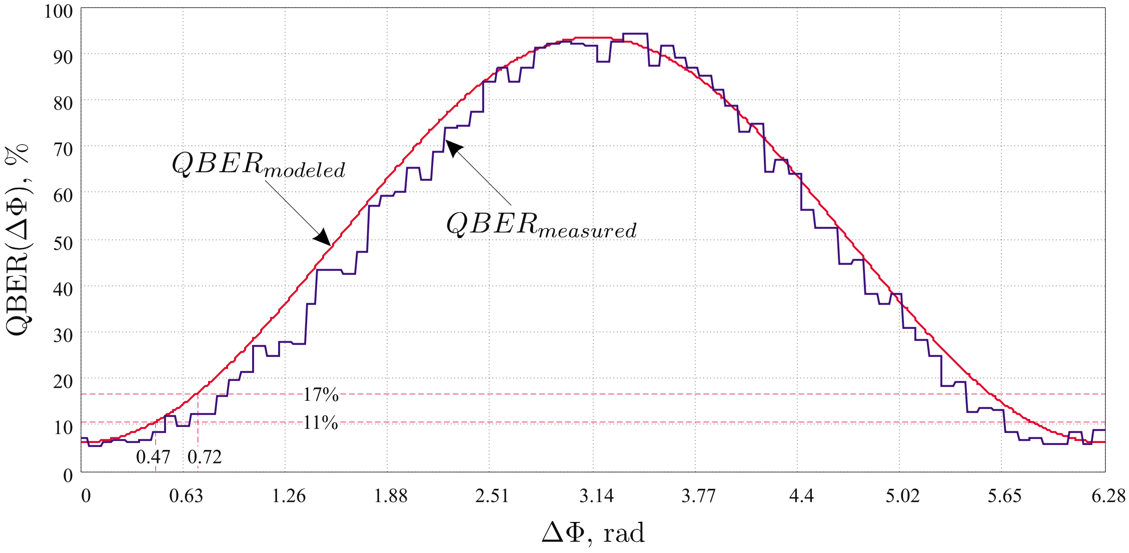

Figure 2. Modeled and measured quantum bit error rate vs. extraneous phase shift angle for the QKD link. The system is usable up to a $QBER_{thresh}$ in the range of 11-17%, but with reduced key throughput. This corresponds to a phase error $\Delta\Phi_{thresh} \approx 27°$-$41°$.

The link is considered operational as long as the QBER stays below some threshold $QBER_{thresh}$, which depends on the Quantum Key Distribution algorithm that is used. Different estimates suggest that the system is usable up to a $QBER_{thresh}$ in the range of 11-17%, but with reduced key throughput. As seen from Figure 2, this corresponds to a phase error of $\Delta\Phi_{thresh} \approx 27°$-$41°$. This range depends on the parameters of the system, such as the dark current noise of the detectors, detector efficiencies, the loss of the fiber between Alice and Bob, receiver efficiency and fringe visibility, and the mean photon number of the source,[3] as well as on the error correction and privacy amplification protocols employed.

In order to compensate for the errors that result from thermally-induced phase changes in the interferometers, we determine the phase error from the statistics related to detection events. We then compensate for the phase error dynamically in real time by adjusting the voltage of a fiber stretcher in the short arm of Bob's interferometer, as shown in Figure 1.

In order to directly separate the extraneous phase error from the intended photon phase values in the detection statistics, we would also need to know the phase shift values applied by Alice for each qubit, $\Phi_{Va} + \Phi_{Ba}$. This information is not immediately available to Bob during data transmission, since the bit value and basis phases transmitted by Alice are completely random. Some of this information becomes available after the sifting of qubits, however, the variation in phase error is typically too rapid to allow for information from the delayed qubit sifting to be useful. Thus we introduce the notion of training frames: such frames contain qubits encoded using deterministic (value, basis) pairs at Alice, as agreed upon by Alice and Bob prior to frame transmission. While receiving qubits in training frames, Bob continues to apply a random basis. However, since the (value, basis) settings of Alice are known apriori to Bob, Bob can recover the total phase shift Φ_0 for each qubit without public communication with Alice. Since the detection probability distribution function for both detectors depends on Φ_0 and phase error, one can estimate the value of the error by solving a set of non-linear equations.

2. DATA FRAMES AND TRAINING FRAMES

In addition to qubits at 1550 nm, Alice also transmits bright pulses at 1310 nm (sync channel), multiplexed on a same fiber, in order to send timing and framing information to Bob (not shown in Figure 1). This includes frame boundaries, type identification and numbering.

In normal operation, the QKD link transports a mixture of data frames and training frames. Data frames convey modulated weak pulses for quantum cryptography. Training frames convey modulated weak pulses for deriving continuous interferometer path-length control signals. These two types of frames are distinguished by the values in their frame type fields, indicated using the bright pulses in the sync channel. Figure 3 shows, in high level form, how these two types of frames are intermixed on the QKD link. At present, we send a repetitive pattern of N data frames followed by M training frames, and the duty cycle of the training frames $d = M/N$ is equal to 2%. While d is fixed here, it could be varied adaptively based on observed link characteristics.

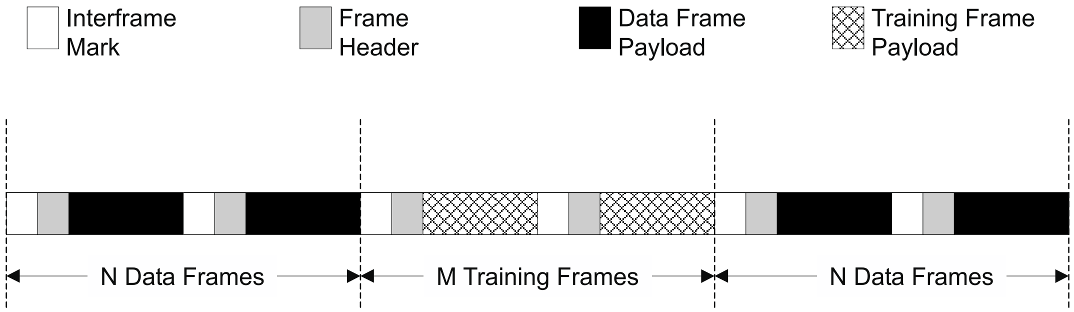

Figure 3. Normal operation alternates sequences of data frames and training frames.[4]

Figure 4 depicts two different approaches to the training frame payloads, that is, to the dim pulses conveyed within the body of a training frame[*]. In both cases the payload consists of modulated dim pulses, such as those in data frames. In the simpler variant, (a), Alice uses a fixed pattern when modulating the pulses in a training frame payload. In the more complex variant, (b), Alice uses a deterministic but pseudo-random pattern when modulating the pulses, with the frame number as the seed for the pseudo-random number generator of the (basis, value) pairs.

[*] A third approach discards the notion of training frames altogether, and instead sacrifices a select subset of bits within the data frames for training purposes. These bits may be selected by a pseudo-random algorithm in order to make it hard for the eavesdropper (Eve) to determine how much training is being performed or to influence the training.

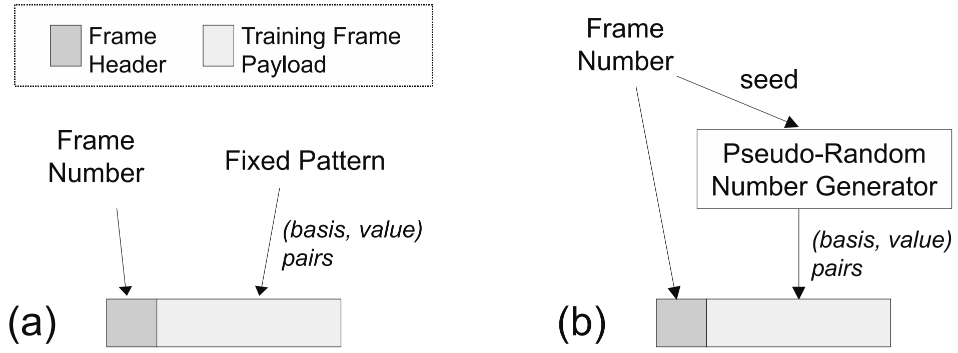

Figure 4. Two different approaches to generating training frame payloads.[4]

Currently we employ the simpler variant (a), which works as follows: for each training frame, Alice prepares a well-known sequence of (basis, value) pairs that are identical for every training frame. In particular, this sequence is a repetition of the following pairs: (0,0), (0,1), (1,0), (1,1), which corresponds to the $\Phi_{Va} + \Phi_{Ba} = 0, \pi/2, \pi, 3\pi/2$.

The more complex variant (b) works as follows: for each training frame, Alice first prepares a frame number and includes that in the frame header. Alice also uses this frame number as a seed for a deterministic algorithm such as a pseudo-random number generator, which in turn generates a sequence of (basis, value) pairs from this original seed. Alice then modulates the training frame's dim payload pulses using this derived sequence. After Bob has received the frame, Bob can extract the frame number and run the same deterministic algorithm in order to determine the sequence of (basis, value) pairs that Alice sent within this frame.

In either case, Bob's hardware is currently incapable of deterministically controlling the receiver's basis values in realtime as it receives a training frame. This is because there is a lengthy and essentially uncontrolled delay between when Bob's Optical Process Control (OPC) computer generates a series of basis values in its local memory, and when the corresponding sequence is clocked out from Bob's digital I/O card to control Bob's phase modulator.

As a result, Bob does not attempt to perform any special type of basis-control (phase modulation) for training frames. Indeed, it treats data frames and training frames identically in this regard. However, in either the (a) or (b) variants described above, Bob can determine - without public communication with Alice - what basis values Alice used, because they are deterministic. As a result, Bob can use this knowledge to build the table of counts similar to the Table 1. Since only one training event can happen for each qubit, when counts in Table 1 are normalized to the total number of the events, the joint probability table is obtained and used as input for the path-length control algorithm.

3. A MATHEMATICAL MODEL FOR DETECTION STATISTICS

Experimentally, the receiving of a qubit can be divided into two experiments: setting the interferometer's phase, and observing detector values. As a whole, the sample space of this experiment consists of eight possible combinations of phase settings (four for Alice and two for Bob for classical BB84 protocol), and four combinations of detector values ($D^{(0)} = 0 \cap D^{(1)} = 0$, $D^{(0)} = 1 \cap D^{(1)} = 0$, $D^{(0)} = 0 \cap D^{(1)} = 1$ and $D^{(0)} = 1 \cap D^{(1)} = 1$). This array is more manageable when organized in terms of joint probabilities.[5]

Define two separate experiments, A and B. Experiment A will consist of disjoint events $A_0 \ldots A_7$, each corresponding to the specific total phase shift in both interferometers, $\Phi_0 + \Delta\Phi$, where $\Delta\Phi$ is the extraneous phase error. Experiment B will consist of four disjoint events $B_0 \ldots B_3$, each corresponding to a different combination of the detection events. This leads to a joint probability distribution array as shown in Table 2. The sum of the joint probabilities in any column n will result in the marginal probability $P(B_n)$, which indicates

Table 1. Detection table for binned counts of training events since last report. Blank areas are filled with accumulated event counts corresponding to the position in the array.

Alice (v,b)	Bob (b)	Φ_0	No hit	$D^{(0)}$ hit	$D^{(1)}$ hit	Both $D^{(0)}$ and $D^{(1)}$ hit
(0,0)	0	0				
(0,0)	1	$3\pi/2$				
(0,1)	0	$\pi/2$				
(0,1)	1	0				
(1,0)	0	π				
(1,0)	1	$\pi/2$				
(1,1)	0	$3\pi/2$				
(1,1)	1	π				

the probability of occurrence of a particular event from experiment B, irrespective of the results of experiment A. Similarly we can sum the joint probabilities in the row m to obtain the marginal probability $P(A_m)$, irrespective of results of experiment B.

Table 2. Joint probability table for experiments A and B.

$A \diagdown B$	Event B_0	Event B_1	Event B_2	Event B_3	Marginal Probabilities
Event A_0	$P(A_0 \cap B_0)$	$P(A_0 \cap B_1)$	$P(A_0 \cap B_2)$	$P(A_0 \cap B_3)$	$P(A_0)$
Event A_1	$P(A_1 \cap B_0)$	$P(A_1 \cap B_1)$	$P(A_1 \cap B_2)$	$P(A_1 \cap B_3)$	$P(A_1)$
.	.	.	.	.	.
.	.	.	.	.	.
.	.	.	.	.	.
Event A_7	$P(A_7 \cap B_0)$	$P(A_7 \cap B_1)$	$P(A_7 \cap B_2)$	$P(A_7 \cap B_3)$	$P(A_7)$
Marginal Probabilities	$P(B_0)$	$P(B_1)$	$P(B_2)$	$P(B_3)$	$\sum = 1$

If we ignore the case when two photons are emitted from the photon source, it can be shown[3] that the probabilities of events B_1 and B_2 can be modeled from the parameters of the system as:

$$P(B_1|\Phi = \Phi_0 + \Delta\Phi) = P(D^{(0)} = 1 \cap D^{(1)} = 0|\Phi = \Phi_0 + \Delta\Phi) = \alpha^{(0)} + \beta^{(0)}\frac{1 + V\cos(\Phi_0 + \Delta\Phi)}{2}, \tag{1}$$

$$P(B_2|\Phi = \Phi_0 + \Delta\Phi) = P(D^{(0)} = 0 \cap D^{(1)} = 1|\Phi = \Phi_0 + \Delta\Phi) = \alpha^{(1)} + \beta^{(1)}\frac{1 - V\cos(\Phi_0 + \Delta\Phi)}{2}, \tag{2}$$

where parameters $\alpha^{(j)}$, $\beta^{(j)}$ and V are offset, scale and visibility parameters of the setup that do not depend on Φ_0 or $\Delta\Phi$. Notice that the conditional probability $P(B_1|\Phi = \Phi_0 + \Delta\Phi)$ on the left side of equation (1) can be determined as the ratio of the joint probability $P(B_1|A_m) = P(B_1 \cap A_m)/P(A_m)$, where A_m is one of the disjoint events $A_0 \ldots A_7$, each corresponding to the specific total phase shift of both interferometers, $\Phi_0 + \Delta\Phi$. Thus we have sixteen non-linear equations, eight for the detection event B_1 and eight for the detection event B_2, with five unknown parameters, $\alpha^{(0)} + \beta^{(0)}/2$, $\alpha^{(1)} + \beta^{(1)}/2$, $\beta^{(0)}V/2$, $\beta^{(1)}V/2$ and $\Delta\Phi$, and one input variable, Φ_0. Using a Gauss-Newton method with Levenberg-Marquardt modifications for global convergence, the least squares estimates of $\Delta\Phi$ can be obtained. This iterative method starts with the initial guess of the unknown parameters. Each iteration adjusts the current guess until the algorithm converges, minimizing the sum of the squared differences between the observed responses (normalized probabilities from the joint probability table) and their fitted values.

In order to determine the initial estimate of the unknown parameters that is required for the iterative nonlinear technique, we consider equations (1) and (2) separately. Both equations are essentially linear in terms of the new parameters, $k^{(j)}$, $x^{(j)}$ and $y^{(j)}$ since:

$$\begin{aligned} P(j,\Phi_0) &= \alpha^{(j)} + \beta^{(j)}\frac{1+(-1)^j V\cos(\Phi_0+\Delta\Phi)}{2} && (3)\\ &= \alpha^{(j)} + \beta^{(j)}\frac{1+(-1)^j V\Big[\cos(\Phi_0)\cos(\Delta\Phi)-\sin(\Phi_0)\sin(\Delta\Phi)\Big]}{2} && (4)\\ &= k^{(j)} + (-1)^j\Big[\cos(\Phi_0)x^{(j)} - \sin(\Phi_0)y^{(j)}\Big], && (5)\end{aligned}$$

where,

$$\begin{aligned} x^{(j)} &= V\beta^{(j)}\cos(\Delta\Phi)/2, && (6)\\ y^{(j)} &= V\beta^{(j)}\sin(\Delta\Phi)/2, && (7)\\ k^{(j)} &= \alpha^{(j)} + \beta^{(j)}/2, && (8)\end{aligned}$$

and $j = 0, 1$ is the index of the detection events equal to 0 for B_1 and 1 for B_2 events.

Equation (5) is linear, and the unknown parameters can be determined in one iteration by least squares fit, for $j = 0$ and $j = 1$. Once parameters $k^{(j)}$, $x^{(j)}$ and $y^{(j)}$ are obtained, a good initial estimate of $\alpha^{(j)} + \beta^{(0)}/2$, $\beta^{(j)}V/2$ and $\Delta\Phi$ can be obtained from (9):

$$\begin{aligned} \Delta\Phi &= \operatorname{atan2}(y^{(j)}, x^{(j)}),\\ (\beta^{(j)}V/2)^2 &= (x^{(j)})^2 + (y^{(j)})^2,\\ \alpha^{(j)} + \beta^{(j)}/2 &= k^{(j)}. && (9)\end{aligned}$$

Since $\Delta\Phi$ is a common parameter for both detectors, two initial guesses are available. The fit with a smaller residual is more accurate, and thus is a better candidate for the initial guess. Notice that all initial estimates have to be computed only once. For consecutive estimation, the previous estimate of the parameters can be used.

4. FEEDBACK CONTROLLER DESIGN

A feedback loop is required to design a control system that is insensitive to variations and nonlinearities of the components. The overall system diagram is illustrated in Figure 5, which shows a feedback loop consisting of a plant P and a controller C. The purpose of the system is to make the plant variable $\Delta\Phi$ follow the set point r in spite the disturbances l and n that act on the system. The load disturbance l, which is caused by the path-length variation, drives the system away from its desired state of $\Delta\Phi = 0$. The estimation noise n, which results from the errors in estimation, corrupts the information about the system obtained from the nonlinear estimator. The plant of the system, which consists of the phase shifter, the training frames subsystem, and the nonlinear estimator, is essentially a linear system. It is characterized by the proportional gain of the fiber stretcher and sampling dynamics that arise from the delay required to collect data and compute the estimates.

4.1. Modeling Disturbance

4.1.1. Load disturbance

The graph of a typical load disturbance l for our setup is shown in Figure 6. It can be seen that the disturbance is slowly rising, with the maximum rate of change equal to $\sigma_{max} = 0.0086$ rad/sec. Thus, within a small period of time, the differential path-length variation can be modeled as a ramp function with variable slope that changes from zero to σ_{max}. The maximum rate of change depends on the thermodynamic properties of the interferometric

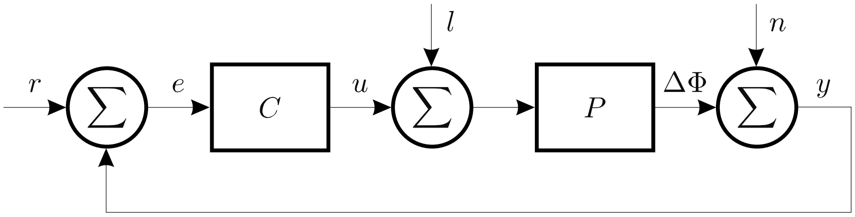

Figure 5. Block diagram of the feedback system for path-length control. The system under control, plant P, has a state variable $\Delta\Phi$ whose measurement y is corrupted by the statistical estimation noise n. The controller C takes inputs from y and setpoint r, and outputs a control signal u that, along with path-length disturbance l, is applied to P.

setup. In our setup, for example, we have used two foam boxes to isolate Alice's and Bob's interferometers, and the maximum rate of 0.0086 rad/sec corresponds to an experimental measurement with the isolating boxes in place in a lab environment. One might obtain a better rate by isolating both interferometers in smaller packages with the isolation of a large thermal mass.

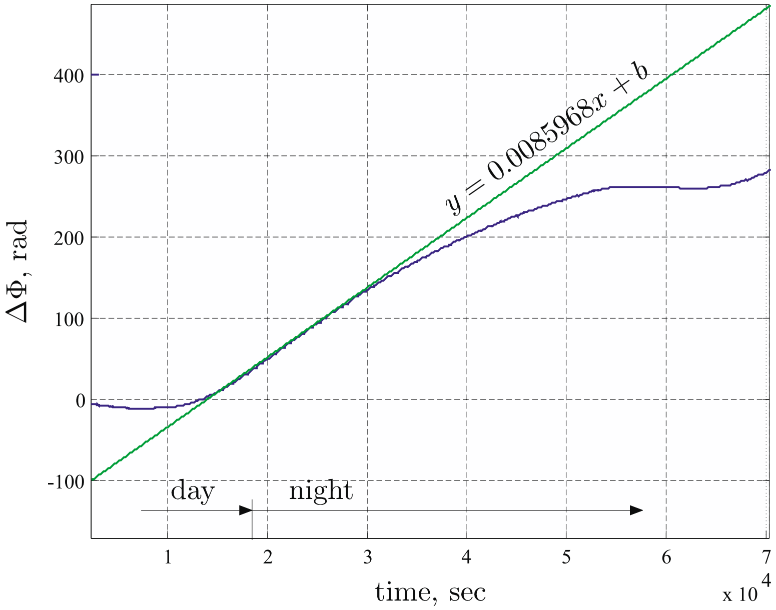

Figure 6. Alice-to-Bob differential path-length variation (load disturbance) over time. The maximum rate of change is observed in the period between 1×10^4 and 3×10^4 seconds and is equal to 0.0086 rad/sec. With this rate it takes about 12 minutes to complete a full cycle of 2π.

The rate of change is one of the parameters that determine the controller's sampling time. First, in order to have a half-degree precision with the above disturbance rate, the final controller must sample at least every second, although this requirement is normally less stringent. Second, the fluctuations in the phase error wash out the observable contrast between the probability estimates obtained from the counting table. Consider that for some qubit k the phase error is $\Delta\Phi_k$. For the next qubit $k+1$, the phase error has changed by $\sigma_{max}/(d \times f)$, where f is the frequency of the transmission and $d = M/N$ is a duty cycle of the training qubits. The nonlinear estimator requires multiple counts in the detection table in order to determine the phase error accurately. Thus the final probability of detection is the weighted sum of the probabilities of multiple photons, each one modulated with a different phase error. As a result, the estimation noise disturbance n depends on the load disturbance l, especially for the large sampling time periods.

4.1.2. Estimation noise

The estimation noise depends entirely on the "quality" of the data used. When the sampling time and training frame duty cycle are chosen such that there are few photon detection events in a counting table for each sample, one might expect high estimation error. Similarly, if the sampling time of the controller is very large (six minutes, for example), the number of the detection events is very high. However, since the resulting probability of detection is corrupted by the path-length variations, the estimation error is high as well. Thus, there is an optimal sampling time period that results in the minimum estimation noise.

Using a mathematical model for detection statistics[3] with parameters measured from the link operating at 1 Mb/s, one may determine how the error in estimation changes as a function of a sampling time period, assuming that the path-length variation is changing as a ramp with $\sigma_{max} = 0.0086$ rad/sec. The graph of this function is shown in Figure 7 for the duty factor $d = 2\%$.

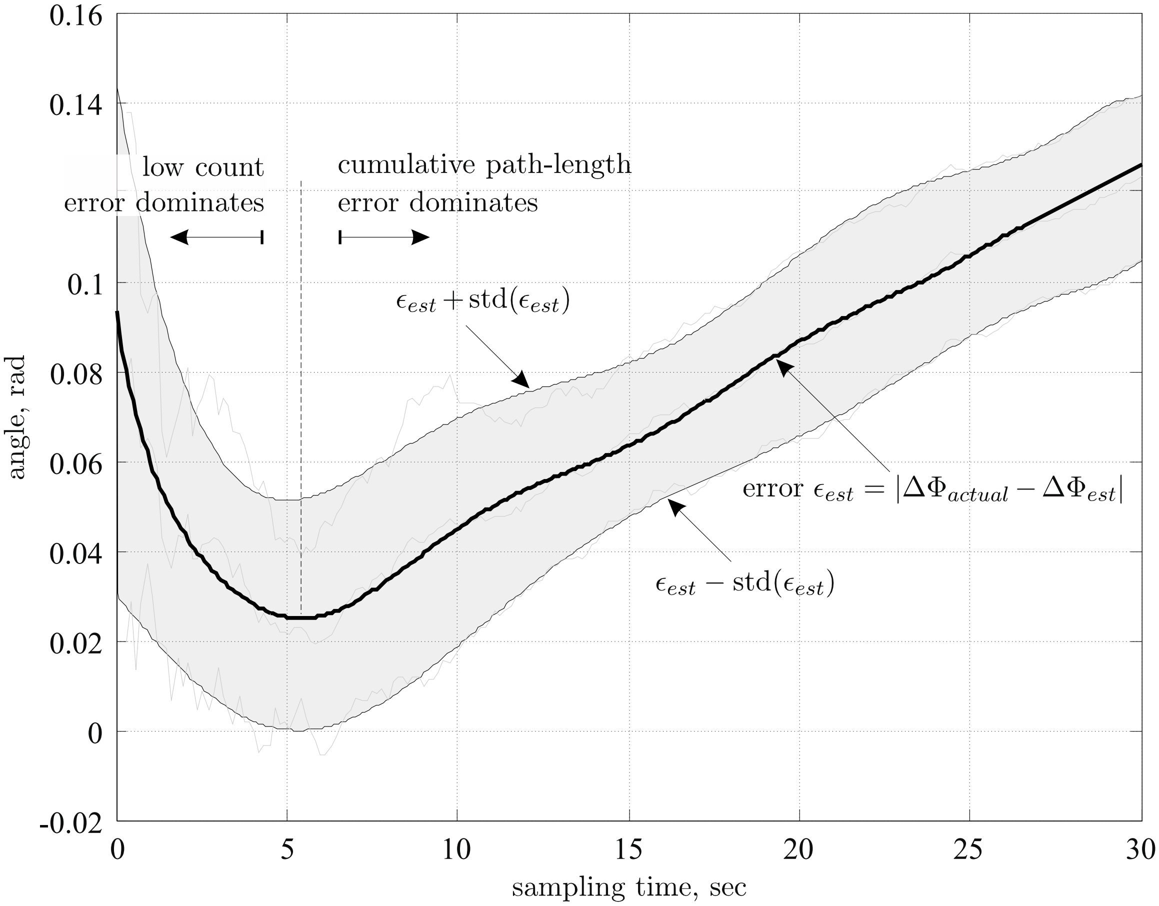

Figure 7. Simulated estimation error, ϵ_{est}, as a function of sampling time. The load disturbance rate is $\sigma_{max} = 0.0086$ rad/sec and the training frame duty cycle is $d = 2\%$. The actual phase error is a ramp function with the initial value of π and the slope of $\pm\sigma_{max}$, $\Delta\Phi_{actual} = \pi \pm \sigma_{max} t$. When the detection table is sampled faster than ≈ 200 msec, it does not contain enough counts and the estimated phase error spikes up (not shown). When the detection table is sampled faster (smaller sampling time) than 6 sec, the low count error is high. When the detection table is sampled slower (larger sampling time) than 6 seconds, the cumulative path-length error dominates the estimation error. The sampling time of 6 sec has the smallest estimation error of $1.5 \pm 1.5°$.

As expected, there are two sources of error in estimation: the low-count error that arises from the discreet nature of the detection events, and the cumulative path-length variation error, as described in a previous section.

When the sampling period is very small, on the order of 200 ms, there are no counts in the detection table and the phase error cannot be estimated. When the sampling time period is in the range of 1-6 sec, the low-count error dominates, since there are only a few counts in the detection table. At higher sampling time periods, the number of detection events is high and the cumulative effect of the path-length variations begins to dominate the estimation error. The optimal sampling time of 6 sec has the smallest estimation error of $1.5 \pm 1.5°$.

4.2. Controller Design

4.2.1. Design constraints

At this point we are ready to summarize the design constraints for the controller C. Since the load disturbance can be approximated with a ramp, we would like to have a system with a zero steady-state error for a ramp input. We would also like to have a reasonable settling time (<60 sec) and overshoot (<50%) for a step input (initial startup of the system), and a small overshoot for the ramp input with a slope σ_{max}. As a rule of thumb, in order to have good stability and robustness, it is desirable to have a gain margin above 8-dB and a phase margin above 50°. The last requirement is obtained from experience and can be justified mathematically only to certain extent.[6]

The sampling time of 6 seconds has the smallest estimation error of $1.5 \pm 1.5°$, as shown in Figure 7. This error applies to the phase error immediately after the fiber stretcher voltage is adjusted for each sample. However, we are also interested in the average error for the qubits between samples, ϵ_{ave}, which can be approximated as $\epsilon_{ave} = 0.5 \times \sigma_{max} \times t$ for the ramp load disturbance. The graph of a total error, $\epsilon_{total} = \epsilon_{ave} + \epsilon_{est}$ is presented in Figure 8. When t is small, the average error is close to zero, but the estimation error is high. The sampling period in the range 2.5-5.5 sec results in the small total error of $3 \pm 1.5°$. The sampling period of the controller is chosen to be $T_{sample} = 4$ sec, which corresponds to the minimum total error. A good rule of thumb is to let the desired closed-loop bandwidth of the feedback system to be at least 5 times slower than the sampling frequency, in order to avoid sampling problems. The closed-loop bandwidth, gain cross-over frequency, and phase cross-over frequency of the system can be assumed roughly the same, $\omega_B = 1/5 \times 2\pi/T_{sample} \approx 0.3$ rad/sec.

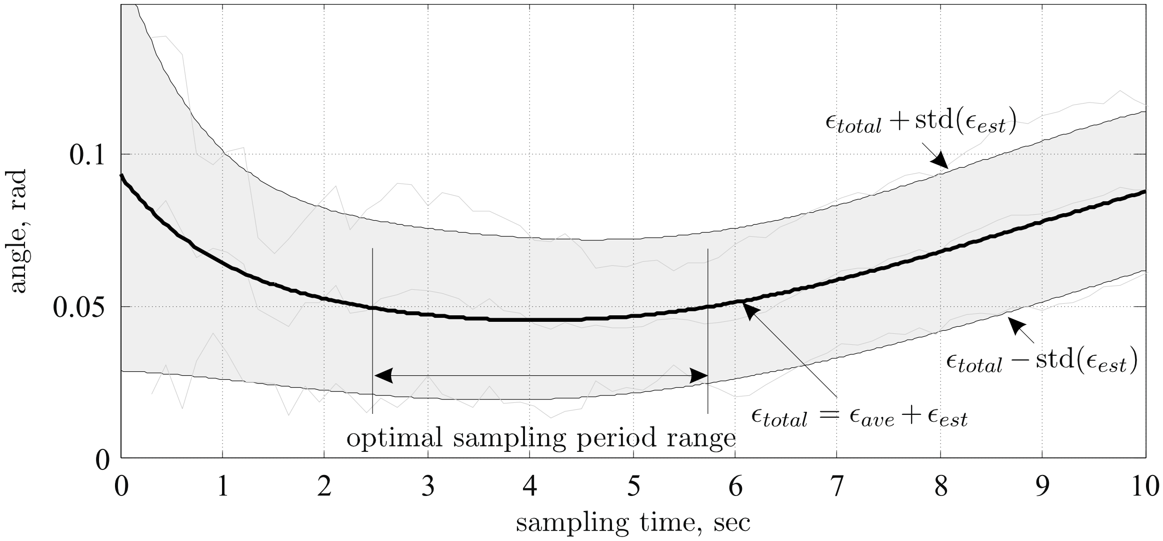

Figure 8. Simulated total error, $\epsilon_{total} = \epsilon_{ave} + \epsilon_{est}$, as a function of sampling time. The load disturbance rate is $\sigma_{max} = 0.0086$ rad/sec and the training frame duty cycle is $d = 2\%$. When $t < 1$ sec, the average error is close to zero since the phase value is updated frequently, but the estimation error is high. When $t > 7$ sec, the estimation error is low, but the average error is high. The optimal sampling period range is between 2.5 and 5.5 sec, with the minimum total error of approximately $3 \pm 1.5°$ at 4 sec.

4.2.2. Design procedure

The transfer function of the fiber stretcher, training frame system, and nonlinear estimator can be approximated as a unit delay, $P = 1/z$. We can use the combination of root locus and pole placement design methods, as shown in Figure 9. We start by designing a discreet time controller with a double integrator, by adding two controller poles at 1. The presence of the double integrator in the transfer function will guarantee a zero steady-state error for the ramp input.

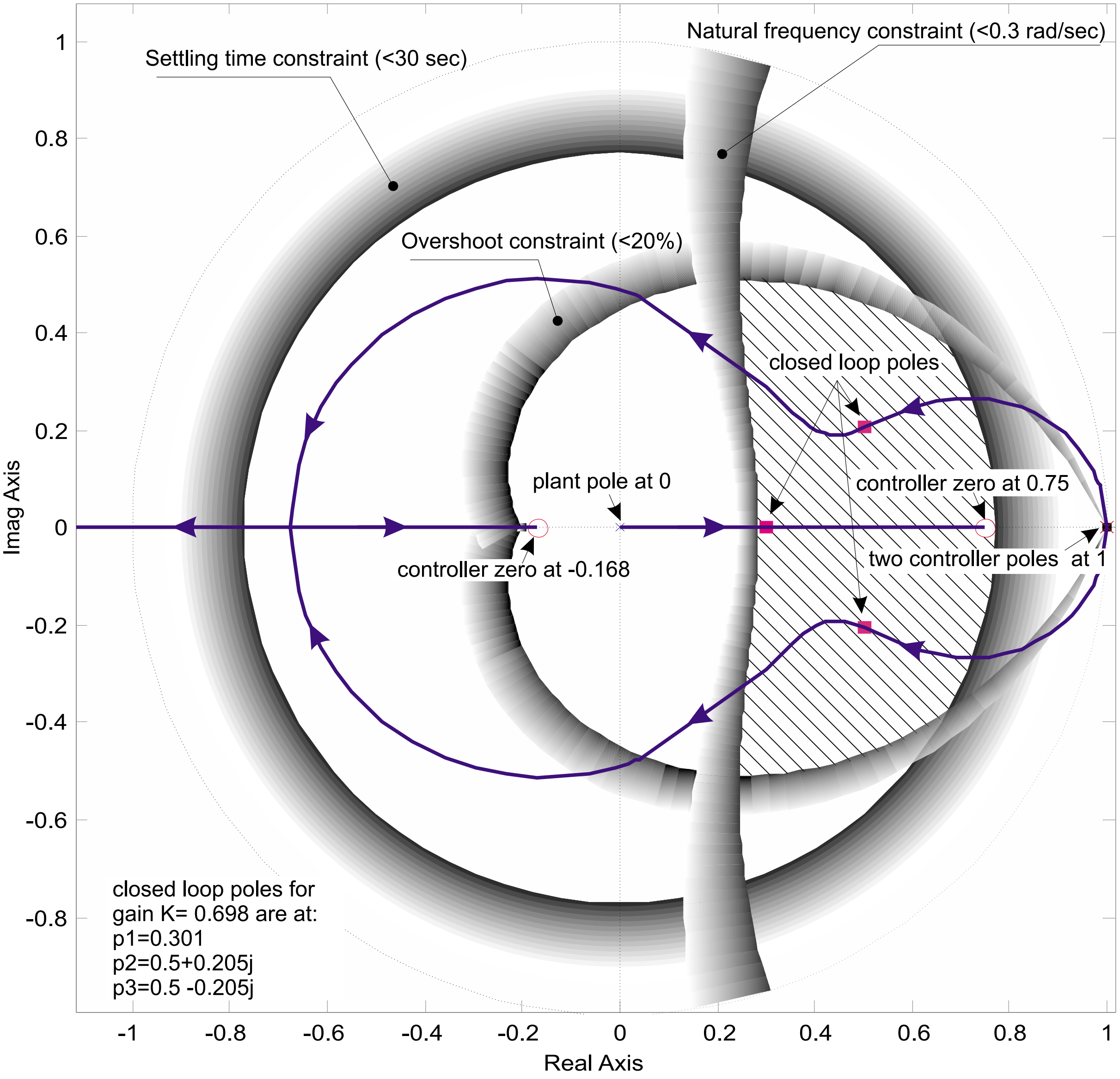

Figure 9. Root locus of the closed-loop path-length control system. The transfer function of the plant is just a unit delay with a pole at 0. Two controller poles are placed at 1 in order to achieve a zero steady-state error for the ramp input. One controller zero is placed at 0.75 in order to stabilize the closed-loop system. The second zero is placed at -0.168 in order to satisfy other design constraints. The hatched region shows the area where the settling time, natural frequency and overshoot constraints are satisfied. The closed-loop poles of the system are placed within this region at $p_1 = 0.301$, $p_{2,3} = 0.5 \pm 0.205j$.

The first zero of the controller is placed at 0.75 in order to stabilize the system. The second zero of the controller is placed at -0.168 in order to satisfy the closed-loop bandwidth, settling time and overshoot constraints, which are shown in Figure 9 as well. The hatched area is the region where all three constraints are satisfied. The closed-loop poles of the system are placed within this region for the proportional gain 0.698 and $p_1 = 0.301$, $p_{2,3} = 0.5 \pm 0.205j$. The corresponding damping and natural frequency for the last two poles is $\zeta = 0.845$ and $\omega_n = 0.182$ rad/sec. Assuming that the first two poles are dominant, this corresponds to the phase margin of approximately 84.5°. The frequencies of all three poles are at least five times lower than the desired sampling frequency of 4 sec to avoid sampling problems. The final controller is:

$$H(z) = 0.698 \times \frac{(z+0.168)(z-0.75)}{(z-1)^2}. \tag{10}$$

The simulation results for the closed-loop system yield the following dynamic characteristics:

- 35.2% overshoot for a step input;
- 24 sec settling time (14%) for a step input;
- 0.045 rad peak value for a ramp load disturbance with a slope σ_{max};
- 73° phase margin at 0.287 rad/sec;
- 9.35 dB gain margin at 0.785 rad/sec.

We implemented this controller in LabVIEW[7] using a cascade method. A programmable voltage source with a standard IEEE-488 interface was used as a D/A converter of the output controller voltage. The measured step response of the system is shown in Figure 10. At time $t_1 = 100$ sec we applied the step input of π rad. After the phase shift of π is established, we returned the set point to zero in order to estimate the maximum settling time of the system.

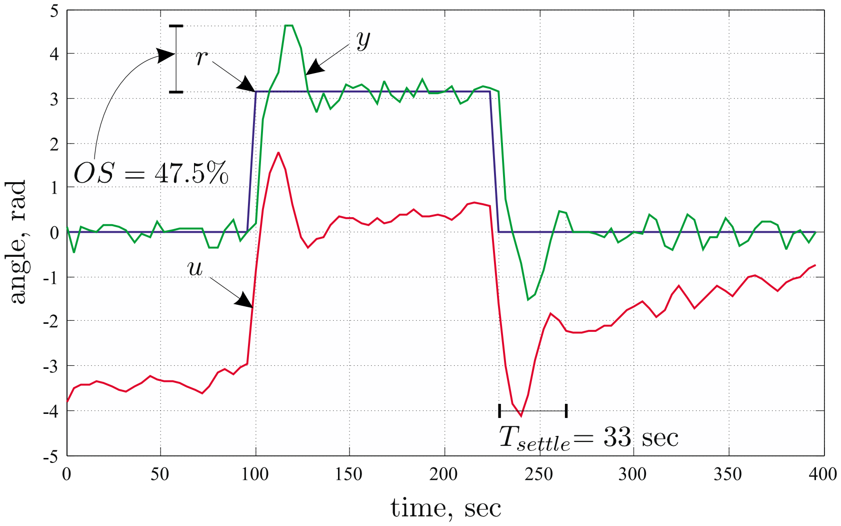

Figure 10. Measured step response of the closed-loop path-length control system. Waveforms r and u are setpoint and control signals of the system, y is the observed phase error (observed state). At $t = 100$ sec the phase error setpoint, r, was changed to π rad, driving the system completely out of phase. At $t = 225$ sec the setpoint was returned to zero to observe system's settling time.

The actual dynamic characteristics from Figure 10 are as follows:

- $OS = 47.5\%$ overshoot for a step input;
- $T_{settle} \approx 33$ sec settling time for a step input (14%).

The difference between simulated and measured values can be partially accounted for by the additional delays in the actual system introduced by the time required to compute and update the new control output. This results in higher overshoot (47.5% vs. 35.2%) and longer settling time (33 sec vs. 24 sec).

Figure 11 shows the normal operation of the path-length controller after start-up. The average steady-state error of the observed system state y is zero, even though the load disturbance is a slow ramp, as seen from the control signal u. It should be noted that the fiber stretcher[†] is chosen such that it can contribute a total phase shift from -2π to $+2\pi$. Thus, when the controller reaches the end of this range, the control signal u is stepped back by the factor of $2\pi \approx 5$V. The total measured QBER is $7 \pm 1.5\%$.

The estimation noise in the actual system is significantly higher than in the simulated results in Figures 7 and 8. This is due to the additional sources of randomness, such as the random basis at Bob and the random nature of the detection events in avalanche photodiodes, not included in the simulator. As the training frame duty cycle is increased from $d = 2\%$ to $d = 50\%$, the variance in the phase error estimate decreases, however, the variance in total QBER stays constant, std(QBER) $\approx 1.5\%$. This is because the estimation noise frequency for this range of d is greater than the cross-over frequency of the controller. Therefore, the controller acts as a low-pass filter for the phase error estimate. At $d = 1\%$ the standard deviation in measured QBER increases significantly, std(QBER) $\approx 5.5\%$, and at $d = 0.5\%$ the controller has almost no information about the phase error and the average QBER becomes approximately 20%.

There is a trade-off between reducing the settling time, T_{settle}, which results in a higher cross-over frequency of the system, and reducing the training frame duty factor, d, which results in a high-frequency estimation noise. At present, both parameters are fixed. Ideally, however, only training frames are transmitted ($d = 100\%$) when large transients are expected, such as at system startup or during switching, and within this time the controller adapts to minimize the settling time of the system. Once the steady-state value of the phase error is reached, the number of training frames is reduced, and the controller automatically adapts to minimize the estimation noise error.

5. CONCLUSIONS

The path-length control mechanism used in our phase-encoded QKD link allows for uninterrupted transmission of the quantum key bit material by sacrificing very little (2%) data bandwidth to the training frames used to measure differential path-length. This is a significant step in making such system practical and fieldable. Although we have used a separate fiber stretcher to keep Mach-Zehnder interferometers at Alice and Bob precisely matched despite environmental disturbance, the same approach can be used to adjust the path-length via a control voltage applied to the phase shifter at Bob.[8]

We have shown that there is an optimal sampling time, which can be determined specifically for a given setup. In order for the controller to work on other QKD links, or on a configuration with fluctuating parameters, it would be necessary to adjust the sampling time or the duty cycle of the training frames dynamically.

The path-length controller of the system is designed using classical control methods and can be tuned to satisfy a variety of design constraints with a deep insight on system behavior. Another alternative is to use Kalman filtering to estimate the phase error. This approach has an advantage over the nonlinear least squares estimator, since it accounts for the prior knowledge about the phase error via a recursive process.

[†] Canadian Instr. Research Fiber Stretcher Model 915, 4 turn 1550 PM fiber

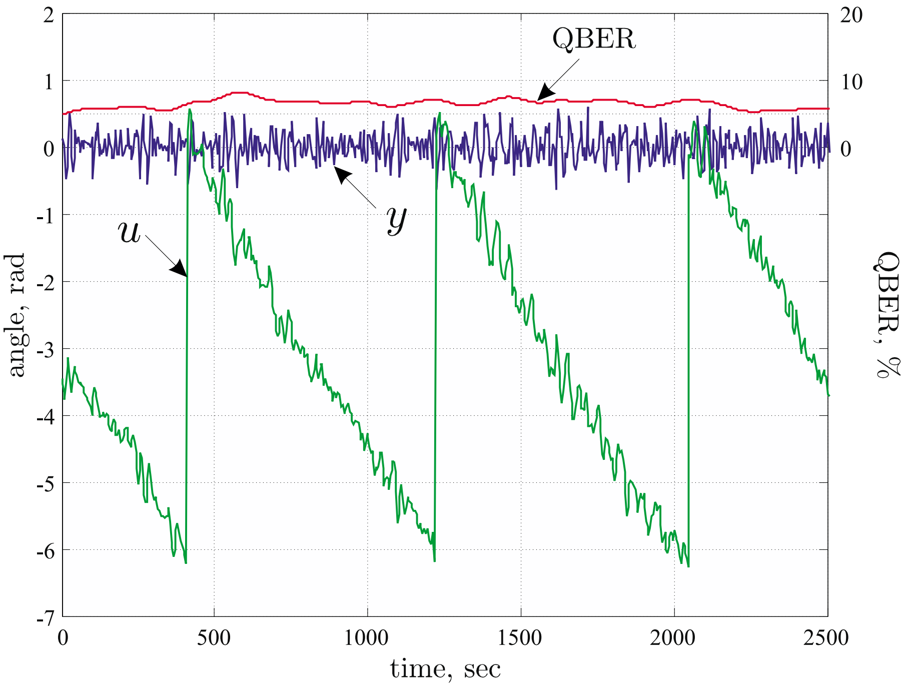

Figure 11. Normal operation of the path-length control system with an extraneous phase shift of about 0.0086 rad/sec. The average observed phase error, y, is zero and average QBER (averaged over 20 samples) is about 7%. The control signal, u, wraps around every 750 sec with no apparent affect on y or QBER.

REFERENCES

1. P. Townsend, J. Rarity and P. Tapster, *Single photon interference in a 10 km long optical fiber interferometer*, Electron. Lett. 29, 1993.
2. R. Hughes, G. Morgan and C. Peterson, *Quantum key distribution over a 48-km optical fiber network*, J. Mod. Opt. 47, 2000.
3. O. Pikalo, *A Mathematical Model for Detection Statistics*, to be published, 2003.
4. B. B. Elliott, *System Architecture Description*, BBN Technologies, 2002.
5. R. G. Brown and P. Y. C. Hwang, *Introduction to Random Signals And Applied Kalman Filtering*, John Wiley & Sons, New York, 1997.
6. C. L. Phillips and R. D. Harbor, *Feedback Control Systems*, Prentice Hall, Upper Saddle River, 2000.
7. *LabVIEW User Manual*, National Instruments Part Number 320999C-01, 2000.
8. A. Brylevski, *Quantum key distribution: Real-time compensation of interferometer phase drift*, NTNU Department of Physical Electronics, 199X.