Delayed-choice quantum cryptography

Evan Jeffrey, Matthew Brenner, and Paul Kwiat

Department of Physics, University of Illinois, 1110 W Green St, Urbana, IL, USA 61801

ABSTRACT

Quantum cryptography is a method of communicating securely, the secrecy of which is guaranteed by the laws of physics and information theory. Current implementations suffer from relatively short ranges and low data rates. We are developing a system that modifies the usual protocol by incorporating elements of special relativity. The result is that in principle, *every* detected photon can be used in the final key, thus doubling or tripling the possible data rate. Our delayed-choice quantum cryptography (DCQC) system works by storing the photon sent to Bob in a low-loss optical delay line until a classical signal from Alice informs him which measurement basis to use.

1. "STANDARD" QUANTUM CRYPTOGRAPHY

1.1. Classical Roots

Encryption is the science of encoding messages (called the plaintext) in a form (the ciphertext) that provides no information to unintended recipients, yet can easily be decoded into the original message by the intended recipient. Algorithms for encrypting data date back thousands of years,[1] but only since the advent of modern information theory[2] have useful formalisms been developed for analyzing ciphers. As a result, the past century has seen the emergence of encryption algorithms such as the DES (data encryption standard), RSA (Rivest, Shamir, and Aldeman cipher), and the new AES (advanced encryption standard), that stand up to concerted attacks by intelligent and well equipped adversaries. However, almost all of these algorithms are merely "hard" to crack (that is, recover the plaintext without having the key needed for decryption), where the cipher chosen is based on what an acceptable definition of "hard" is. Furthermore, the security of an algorithm is only ever evaluated based on known attack strategies. Thus, these systems are potentially vulnerable to breakthroughs in analysis techniques, rapid advances in available computing power, and the emergence of new types of computers that follow fundamentally different rules.

For example, the DES, a 56-bit keyed cipher, was once considered secure enough for most any task, yet now can be cracked via brute-force methods in a matter of hours by dedicated hardware. DES has also been shown to be vulnerable to two new powerful analysis techniques, differential cryptanalysis[3] and linear cryptanalysis.[4] RSA, an algorithm based on the difficulty in finding large prime factors, has been losing ground to frequent advances in state-of-the-art factoring algorithms. Moreover, the prospect of quantum computers looms on the horizon, promising to factor numbers fast enough to make RSA trivially crackable. Clearly, then, for secrets which must be kept for "as long as men are capable of evil,"[5] there is a desire for a system secure against not only presently known attacks, but all possible future forms of attack.

One – and only one – provably secure encryption algorithm does exist: it is the "one time pad" (OTP) protocol, which is also one of the simplest algorithms in use. If the sender (from here on, Alice) and receiver (Bob) share a secret string of random numbers of the same length as the plaintext, Alice can simply add the two bit-by-bit (or letter-by-letter) and send the result to Bob. Bob can then subtract the secret key from the ciphertext to recover the original message. The proof of security for this algorithm hinges on the property that for any given ciphertext, *all* possible plaintexts are equally likely, so that the ciphertext contains no information available to a third party. Although OTPs have been used occasionally in espionage and military applications where total security is absolutely necessary, the protocol poses some serious problems. First, it requires a key as long as the message to be sent. This is difficult to achieve in many scenarios. Also, as the name implies, each key (or pad) may only be used once. If it is ever used to encrypt a second message, the security is compromised and both messages could be recovered.

The disadvantages of the OTP make it impractical for most applications, relegating it to be used for short, ultra-secret communications. Even so, the difficulty of key management has sometimes led to OTPs being

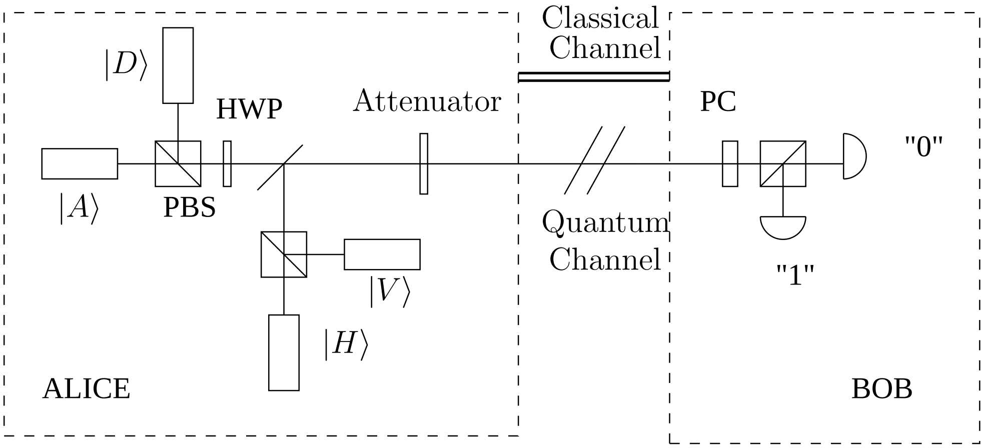

Figure 1. Typical layout for BB84 key exchange protocol. Based on a random number generator, Alice fires one of four lasers, corresponding to the chosen communication states. The resultant pulse is then attenuated to an average intensity of less than 1 photon, and sent to Bob. He randomly selects an analysis basis to measure in, either doing nothing (H-V basis) or turning on a Pockels cell (PC) to rotate the polarization by 45° (D-A basis).

implemented or used insecurely, causing security compromises when a "lesser" cryptography system might have prevailed. No amount of theoretical security can compensate for a poor implementation, so it is desirable to have methods of ensuring that a system is being used properly.

1.2. Protocol

The central problem in the OTP is key distribution – how does one transmit the all-important secret random string of bits from Alice to Bob? Classical key distribution methods, e.g., phone lines or fiber optics, are all potentially vulnerable to an undetected eavesdropper. The heart of quantum cryptography is a quantum key distribution (QKD) protocol that uses "quantum uncertainty" to allow the secure exchange of key material suitable for a OTP by remote parties. The most common protocol for QKD is the BB84 protocol[6] protocol. See Gisin et al. for a superb review of several algorithms and implementations of QKD.[7]

In BB84 (shown in Fig. 1), Alice transmits to Bob a series, not of bits, but of "qubits" (quantum bits). The qubit typically used is the polarization of a single photon. Alice sends qubits randomly chosen from four states $|H\rangle$, $|V\rangle$, $|D\rangle \equiv \frac{|H\rangle+|V\rangle}{\sqrt{2}}$, and $|A\rangle \equiv \frac{|H\rangle-|V\rangle}{\sqrt{2}}$, representing horizontal, vertical, diagonal, and anti-diagonal polarization, respectively. The first two states comprise the H-V basis and the second two comprise the D-A basis. Alice and Bob agree to allow $|H\rangle$ and $|D\rangle$ to represent a logical "0," and $|V\rangle$ and $|A\rangle$ to represent a logical "1." Bob measures the polarization of the photons he receives with an analyzer, randomly oriented to either discriminate between $|H\rangle$ and $|V\rangle$ or between $|D\rangle$ and $|A\rangle$. He then records the outcome for each measurement ("0" or "1"), along with the measurement basis.

Having performed the quantum part of this protocol, Alice and Bob then publicly announce their respective basis choices, but not the actual states they sent or received. Since each basis can represent either logical value, they have not divulged any information about their key data; however, they know that when they used the same basis, their results are perfectly correlated. This is guaranteed because a state prepared as $|H\rangle$ ($|D\rangle$) will never be detected as $|V\rangle$ ($|A\rangle$), and vice-versa. In contrast, when Alice and Bob randomly select different bases, they will get completely uncorrelated results. They now select only the bits where both parties used the same basis, forming the "sifted keys", which are in principle identical. In practice, various noise sources will cause their sifted keys to be slightly different, requiring the use of error correction codes to fix. In addition, they must consider the possibility that an interested third party (Eve, the eavesdropper) may have intercepted, measured, or tampered with the photons "in flight". However, because not all of the states used are orthogonal, if Eve tries to gain information about the polarization of the photons, she will necessarily introduce an error signal. Alice and Bob can detect the errors with error-correcting codes, and use the measured error rate to place an upper bound on

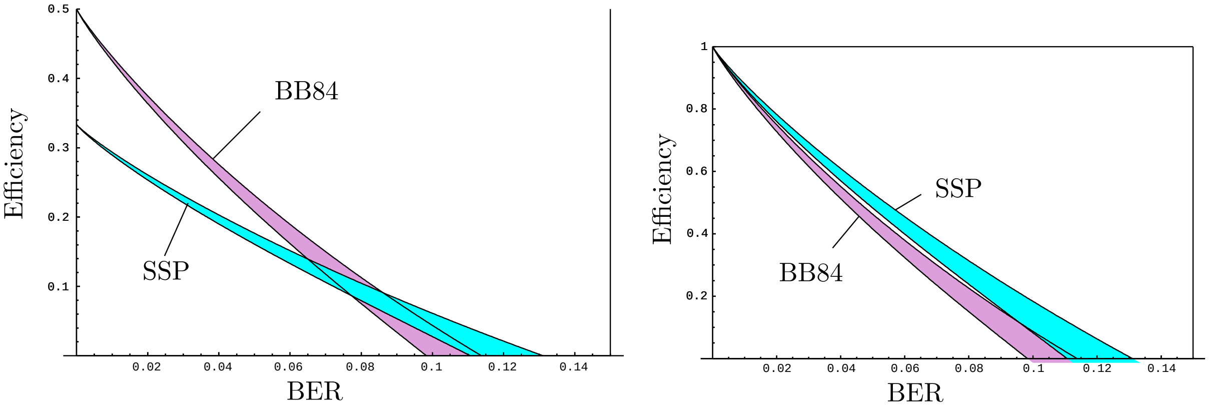

Figure 2. a) Overall efficiency as a function of bit error rate (BER) for the BB84 protocol and the SSP. The width of the bands represents the difference between the best known algorithm and the theoretical limit for error correction and privacy amplification. Note that because of the relative inefficiency in generating the sifted key (the subset of events where Bob measured in the correct basis), only for high BER is the SSP more efficient. b) The same plot, assuming 100% efficiency in sifting, i.e., that Bob *always* uses the correct measurement basis. This is achievable using delayed-choice quantum cryptography.

the amount of information Eve could have obtained. In the final step of privacy amplification, they use hashing techniques to reduce the key down to a length for which Eve has arbitrarily small knowledge, e.g., 10^{-4} bits.[8, 9]

1.3. Six-State Protocol

A variant on the BB84 protocol is the six-state protocol (SSP),[10, 11] which uses *three* bases for communication, for a total of six states. Specifically, we add the R-L basis consisting of the circular polarization states $|R\rangle \equiv \frac{|H\rangle + i|V\rangle}{\sqrt{2}}$ and $|L\rangle \equiv \frac{|H\rangle - i|V\rangle}{\sqrt{2}}$. Since now an eavesdropper can only randomly select the correct basis 1/3 of the time, she will cause a higher BER than with the 4-state protocol. Correspondingly, in the SSP, a given BER (such as from noise) places a lower bound (than in BB84) on the information Eve can have, reducing the quantity of data which must be thrown away during privacy amplification, and thereby increasing the net efficiency in noisy environments. However, since Bob also chooses the wrong basis 2/3 of the time, the maximum efficiency even at low BER is only 33% instead of 50% for BB84. As shown in Fig 2a, unless the BER is greater than $\sim 8\%$ (the exact value depends on the privacy amplification algorithm used), the SSP actually has a *lower* net yield of final secret key bits than BB84. Note, however, that at higher BERs, not only is the SSP more efficient, but there is a range of BERs for which BB84 does not yield any secret key bits, while SSP still does. Put differently, for some BERs, QKD is *only* possible with the SSP.

1.4. Security

The security of QKD rests on an eavesdropper introducing errors in the process of measurement. What Eve would really like is a box that accepts Alice's qubit, copies its state onto a blank qubit, then allows the first to pass on unaltered to Bob. Eve would then simply store the new copy until Alice and Bob publicly exchange the basis information, at which time Eve would correctly measure her copy in the correct basis. Fortunately, Eve's ideal copying device cannot function as she would like, due to the so-called "No cloning theorem"[12]: *The operator* $\hat{\mathbf{O}}$ *which performs the action* $\hat{\mathbf{O}}|\psi\rangle \otimes |0\rangle \equiv |\psi\rangle \otimes |\psi\rangle$ *does not exist.*

$$\text{Consider } \hat{\mathbf{O}}: \qquad \hat{\mathbf{O}}|\psi\rangle|0\rangle \quad \equiv \quad |\psi\rangle|\psi\rangle$$

$$\begin{aligned}\hat{\mathbf{O}}|0\rangle|0\rangle &= |0\rangle|0\rangle \\ \hat{\mathbf{O}}|1\rangle|0\rangle &= |1\rangle|1\rangle.\end{aligned}$$

By the linearity of quantum mechanics,

$$\begin{aligned}\hat{\mathbf{O}}\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)|0\rangle &= \frac{\hat{\mathbf{O}}|0\rangle|0\rangle}{\sqrt{2}}+\frac{\hat{\mathbf{O}}|1\rangle|0\rangle}{\sqrt{2}} \\ &= \frac{|0\rangle|0\rangle+|1\rangle|1\rangle}{\sqrt{2}}.\end{aligned}$$

But, according to the definition of $\hat{\mathbf{O}}$,

$$\begin{aligned}\hat{\mathbf{O}}\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)|0\rangle &\equiv \left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right) \\ &= \frac{(|0\rangle+|1\rangle)(|0\rangle+|1\rangle)}{2} \\ &= \frac{(|0\rangle|0\rangle+|0\rangle|1\rangle+|1\rangle|0\rangle+|1\rangle|1\rangle)}{2}.\end{aligned}$$

$\therefore$ $\hat{\mathbf{O}}$ does not exist, since these two forms are not equivelent.

It can be shown that the error signal gives a bound to the amount of information Eve can gain.[10, 11] If she measures every qubit that passes, the bit error rate (BER) is 25%, which indicates effectively complete knowledge of the shared key, while lower error signals indicate partial knowledge. For sufficiently low error rates, Alice and Bob can cleverly choose to discard data in such a way as to reduce Eve's knowledge of the secret key. This privacy amplification step reduces the usable efficiency of the QKD channel when the BER becomes large. In fact, if the BER is above 15%, there will be no secret key material left after error correction and privacy amplification.[7]

1.5. Assumptions

While quantum key exchange is provably secure if the appropriate error detection, correction, and privacy amplification steps are followed, it is based on a number of assumptions. First, we assume that the public communication channel the parties use to communicate basis choices and error correction information is authenticated. Bob must know that the information he is receiving came from Alice untampered, otherwise Eve can mount a man-in-the-middle attack. For this, she intercepts both the quantum and classical communication destined for Bob and negotiates a key with Alice. Simultaneously, she impersonates Alice to Bob, establishing a quantum key with him.

Second, there is an assumption that Alice can produce single photon Fock states. If Alice unintentionally sends two photons with the same polarization, Eve could remove one photon for later measurement, and transmit the other unmolested to Bob. Her eavesdropping then would be very effective and undetectable from the BER. In practice, most implementations use pulsed laser sources attenuated down to single-photon levels (typically ~ 0.1 photon per pulse). However, the photon number distribution for laser sources is Poissonian – even when the mean photon number per pulse is well below 1, a small but significant fraction of pulses will have two or more photons. Some degree of this can be overcome by attenuating the laser sources further, or with privacy amplification, both at a significant cost in efficiency.

A third major assumption is that the information on the state Alice transmitted must not be available through another channel. In particular, information about the state must not be recorded in any other degree of freedom of the photon, such as frequency or direction, nor may that information be leaked via classical side channels such as RF emission from switches. This may turn out to be one of the hardest requirements to meet.

System noise strongly limits the efficiency of BB84. While Eve must introduce errors to gain information about the key, natural noise sources can also cause errors. To protect their security, Alice and Bob must assume

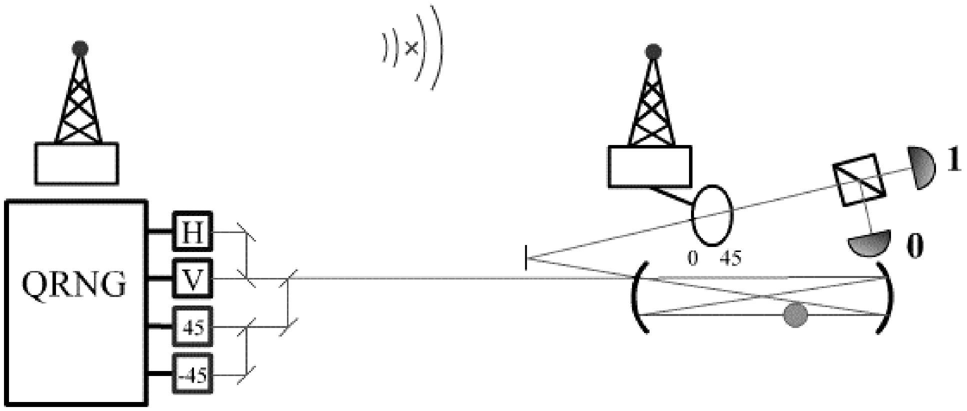

Figure 3. Schematic for delayed-choice system, including the addition of a delay stage for Bob (shown with only 4 passes for clarity) and an extra classical communication component (indicated schematically by the two radio towers, though in practice we implement it using classical laser pulses) for transmitting basis information. The state to send is selected by a quantum random number generator (QRNG).

that *all* errors could be indicating the presence of an eavesdropper, and react accordingly. The efficiency of BB84 will drop in a noisy environment (see Fig. 2, and in a sufficiently noisy environment the protocol will not work at all, as the net yield of secret bits (after error correction and privacy amplification) will drop to zero.

2. DELAYED-CHOICE QUANTUM CRYPTOGRAPHY

In delayed-choice quantum cryptography we seek to remove the inefficiency inherent in sifting the key, by incorporating elements of special relativity. Ordinarily, Alice and Bob would only use the same basis on a fraction of the bits (50% for BB84, 33% for the SSP). The reason for this is that Eve must be unable to gain information on which basis to measure in, effectively precluding Bob from having the same information. In our delayed-choice protocol, instead of measuring his received photon immediately, Bob stores it in his “lab”. Once he has done so, Eve no longer has access to the photon, and Alice is free to broadcast the correct basis to use. Assuming Bob can store photons long enough with high efficiency, he can measure every photon in the right basis, and double the communication efficiency of BB84 QKD, or triple it for the SSP. The fact that Bob and Alice can now in principle use every photon for the key makes the six-state protocol more efficient than the four-state protocol for *any* BER (see Fig. 2b).

2.1. DCQC Protocol

Fig. 3 shows the experimental layout for DCQC. The system is very similar to standard QKD, with the addition of a quantum storage system for storing photons to be measured later, and a fast classical communication system to transmit the basis information to Bob. In our case, the former is accomplished by a delay line constructed from mirrors, while the latter is a laser communication system with low latency modulation. The operation of the system is also similar to standard QKD. As before, Alice sends to Bob a series of photons with polarizations randomly selected from 4 (or 6) states. Bob receives these photons, but instead of measuring them, stores them in the storage device. Once Bob has a photon securely in his lab, Alice sends the information to him on which measurement basis to use. He then measures the photon in that basis, and adds that bit to the secret key. Alice and Bob then perform the usual error correction and privacy amplification steps to generate a final key.

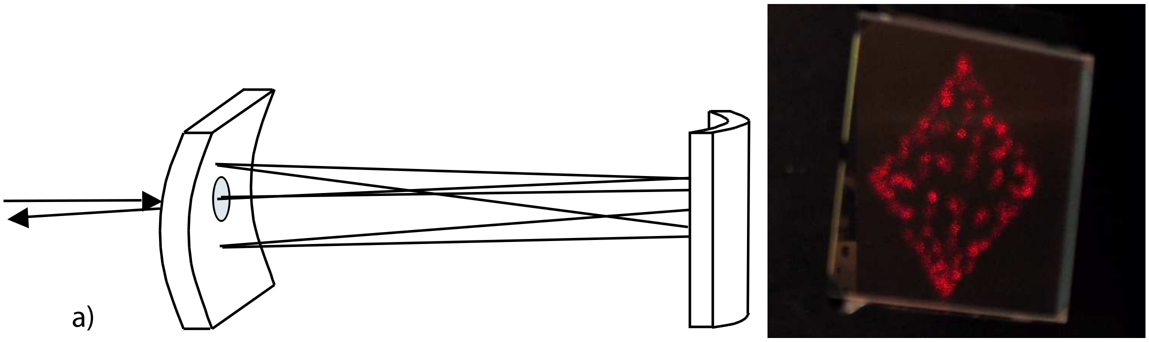

Figure 4. a) Delay line using cylindrical mirrors. By twisting one mirror relative to the other, or slightly adjusting their separation, the number of passes made, and hence the delay time, can be varied. b) photograph of laser spots on one end mirror.

2.2. Quantum Storage System

Bob must store the photon Alice sends him for at least as long as it takes him to process the classical signal and set up his measurement apparatus. Several storage options are possible, e.g., slow light/stopped light systems,[13, 14] or photon-to-atom transduction. However, for a reasonable delay time of 1 μs, the easiest and most efficient system is a long path-length optical delay line. Since 1 μs corresponds to a total length of approximately 330 m, we have designed a folded arrangement, in which light enters the cavity by means of a hole in one mirror, bounces many times between the mirrors, and finally exits via the same hole. Our design is based on the Herriott cells for ring-down spectroscopy.[15] However, whereas these systems typically use spherical mirrors (giving rather limited spot patterns, and short path lengths) or astigmatic mirrors (which are more difficult to manufacture), we employ a pair of cylindrical mirrors, whose axes are intentionally misaligned. The relative orientation is typically 70° to 80°, as shown in Fig. 4. Pittman and Franson[16] have designed an alternative optical delay line.

The behavior of a beam traveling through a system of mirrors can be described using classical ABCD matrices.[17] Each element is represented by a 4x4 operator A which transforms a state vector as

$$A \cdot \begin{pmatrix} x \\ \frac{dx}{dz} \\ y \\ \frac{dy}{dz} \end{pmatrix}. \tag{1}$$

The two important ABCD matrices are for a mirror with given x and y radii of curvature, and for the freespace propagator for a given distance d:

$$\text{Mirror}(r_x, r_y) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ -\frac{1}{2r_x} & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & -\frac{1}{2r_y} & 1 \end{pmatrix} \quad \text{Displacment}(d) = \begin{pmatrix} 1 & d & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & d \\ 0 & 0 & 0 & 1 \end{pmatrix}. \tag{2}$$

From these and a rotation matrix, we construct the ray matrix for one trip through our twisted delay line. A configuration is said to be an N-pass delay line if A^N brings all rays back to their original x and y coordinates, [*] and N is the smallest number for which this is true. If and only if the configuration is stable, the eigenvalues of the ABCD matrix will be complex conjugate pairs with $|\lambda_i| = 1$. We denote these eigenvalues as $e^{\pm i\phi_1}$ and $e^{\pm i\phi_2}$. The reentrant condition for N passes will be achieved when

$$N * \phi_1 = \pi m_x \text{ and } N * \phi_2 = \pi m_y : \{m_x, m_y\} \in \mathbb{Z}. \tag{3}$$

[*] Two classes of delay lines can be constructed, with respect to the output beam. For one class, the output beam is retroreflected along the input path. For the other, the beam exits as if it reflected off the first mirror, i.e., as if there were no entrance hole.

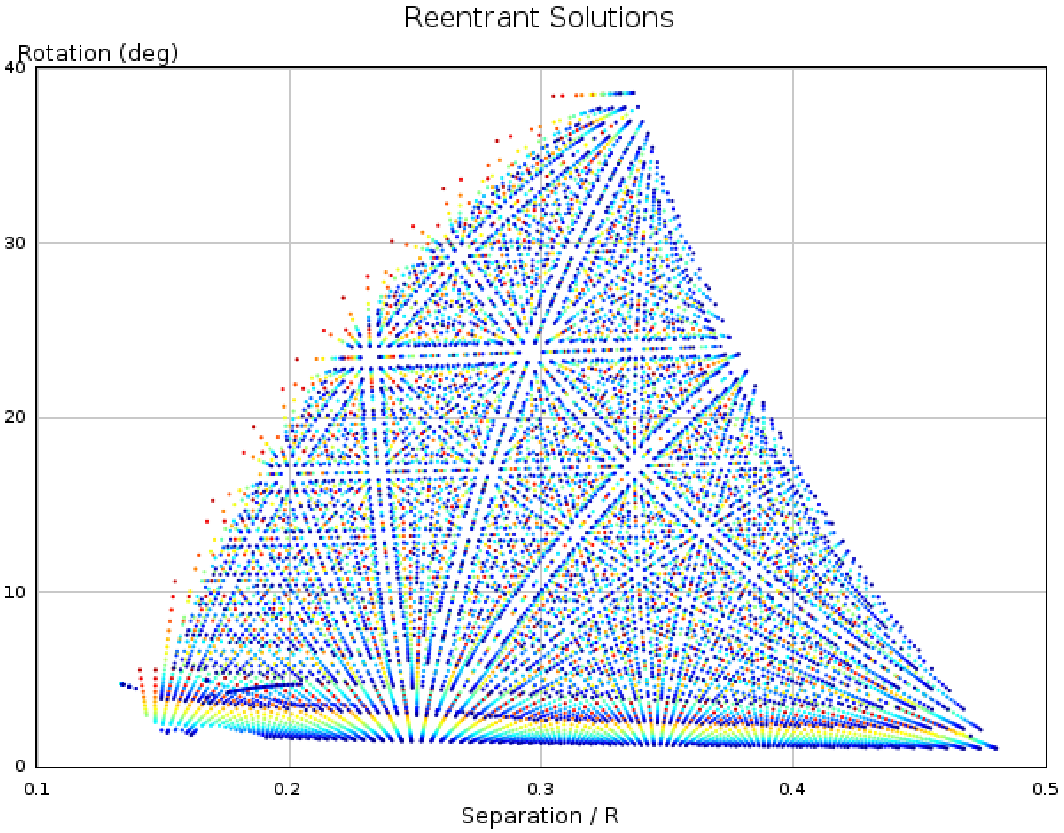

Figure 5. Plot of the reentrant solutions to the ray matrix for a twisted cylindrical delay line. The X axis is the dimensionless base length, defined by the separation divided by the radius of curvature of the two mirrors (assumed to be identical). The Y axis is the twist angle in degrees of one mirror relative to the other. Each point corresponds to a reentrant solution for $40 \leq N \leq 120$, with bluer points indicating more passes and longer delay times, while redder points indicate fewer passes and shorter delay times.

From this constraint, it is possible to select values of N, m_x, and m_y, and then numerically solve to find the separation and relative twist of a pair of cylindrical mirrors that give the desired eigenvalues. Fig. 5 shows the set of solutions for $40 \leq N \leq 120$.

In our implementation we use cylindrical mirrors with a ∼5-m radius of curvature, which gives us a base path length of approximately 2 m. Thus, about 85 round trips through the delay line are required per microsecond of total delay time. This can be achieved with a 15° twist angle. We couple in and out of the delay line through a 6-mm hole drilled in the center of one of the mirrors. The size of the hole is chosen to be large enough to admit a beam whose Rayleigh range is about twice the base length of the delay line without significant diffractive losses. The mirror must be large enough for the nearby spots to be far enough from the coupling hole that the photon does not leak out prematurely.

We have designed and constructed a delay line with a delay time of 960 ns (80 round trips through the delay line of 2-m path length). The total transmission efficiency was $< 20\%$ which is not high enough to make DCQC worth implementing (since it is higher than the loss from sifting). The majority of our losses come from leakage through the mirror coatings; the reflectivity of the mirrors in our prototype system is only 98.9% at the wavelength we are presently using (670 nm). By employing mirrors with reflectivity over 99.99%, we expect to achieve storage losses less than 2%. Some amount of loss comes from clipping and diffraction when going through the coupling hole, which was sized too small in our prototype. We calculate that with a hole diameter 6 times the $1/e^2$ radius of the input beam (assumed Gaussian TEM_{00}) this diffraction loss should be less than 1%.

2.3. Basis Communication

After transmitting the qubit photon, Alice must communicate the basis selection to Bob quickly enough to allow him to perform the measurement within the limits of his storage system. To do this, low latency communication is necessary. To this end, we have designed a fairly fast laser communication system to transmit the basis information. The transmitter consists of a standard laser diode, impedance-matched to be driven directly from a 50Ω pulse generator. The transmitter is driven by a logic circuit implementing a finite state machine (FSM) which accepts a signal on one of 2 (for BB84) or 3 (for the SSP) inputs, each corresponding to a basis, and translates that to a modulation pattern that drives the laser diode. The receiver is a fast photodiode connected to a similar logic circuit that demodulates the signal into 2 or 3 indicators. The output of the receiver is used to trigger a Pockels cell to set the polarization analysis basis.

We designed and built a prototype of the modulation/demodulation circuitry from discrete TTL logic. It functioned as expected at low clock speeds, but with discrete logic, only functioned reliably below 35 MHz, giving a communication delay of at least 260 ns. This is an acceptable, but costs us a large portion of our maximum latency (1 μs). We therefore are reimplementing the logic in a programmable logic device (Xilinx CPLD XC9536) to allow us to increase clock rates further and reduce the communication latency.

2.4. Polarization Analysis

For the four state version of DCQC, polarization analysis is performed using a polarizing beam splitter (PBS) preceded by a Pockels cell. The Pockels cell sets the measurement basis according to the applied voltage. No voltage gives zero net birefringence, and therefore no rotation, so the photon is measured in the H-V basis. If a "half-wave" voltage (typically about 1 kV) is applied, the induced birefringence is the equivalent of a half waveplate, giving rotation by 45° to measure in the D-A basis. One of the main advantages of the delayed-choice system, however, is the ability to efficiently implement the 6-state QKD protocol. We have thus developed a system to measure polarization in three bases using a *single* Pockels cell, rather than the two electro-optic devices that one might believe would be necessary.[18] As shown in Fig. 6, a unitary rotation by $\frac{2\pi}{3}$ about the $(1, 1, 1)$ axis (i.e., the direction equidistant from $|H\rangle$, $|D\rangle$, and $|R\rangle$) in the Poincaré sphere performs a cyclic permutation on the $|H\rangle$, $|D\rangle$, and $|R\rangle$ states, while a negative rotation performs the opposite permutation. With a fixed waveplate and a single Pockels cell with which we can apply either a positive or negative rotation, we can realize a single switch version of the 6-state protocol.

3. DISCUSSION

Like the BB84 protocol, the security of DCQC can be shown to be guaranteed by the laws of physics and mathematics. While BB84 rests solely on quantum mechanics and information theory, DCQC also depends on special relativity. The space-time diagram of Fig. 7 illustrates this point. As long as the past light cone of the arrival of a photon to Bob's laboratory does not overlap the future light cone of Alice's broadcast of the basis choice, no observer constrained by special relativity can have access to the quantum state and the measurement information simultaneously. This means that those two events are space-like separated, so that in some reference frame, Alice does not transmit the classical basis information until *after* Bob has received the photon. Alice and Bob must take care to ensure the space-like separation of the photon-receive event and the send-basis-info event.

Another way to understand the DCQC security is in direct analog to the BB84 logic. In both protocols, Alice publicly announces the basis information. In BB84 this announcement comes just after Bob has measured the photon; in DCQC the announcement comes just before. But, from the perspective of Eve, *these two situations are entirely equivalent*: the reduced density matrix describing Eve's measurement system cannot depend on whether Bob has actually performed his measurement or not. If it could, then Bob and Eve could set up a faster-than-light communication system and leave Alice in wonderland. Therefore, since Eve's information cannot depend on when Bob makes his measurement, the standard BB84 security proofs hold.[19, 20]

There are a number of attack strategies that Eve could use which must be accounted for and protected against. If Alice and Bob rely on the propagation speed of their signals being c to ensure the correct causality,

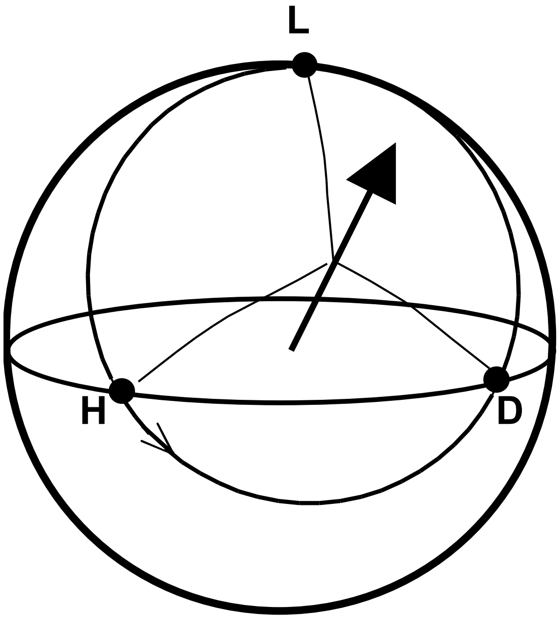

Figure 6. Poincaré representation of polarization qubit. A unitary operator is specified by an axis an angle of rotation. In this case, rotating around the $(1, 1, 1)$ axis as shown by $\pm\frac{2\pi}{3}$ allows us to rotate either $|D\rangle$ or $|R\rangle$ to $|H\rangle$ for measurement by a PBS. Birefringent elements such as Pockels cells usually rotate only around an axis on the equator of the Poincaré sphere, so we use a fixed waveplate in front of the Pockels cell to make it effectively rotate around an inclined axis.

an eavesdropper who can arbitrarily delay the quantum *and* the classical channels could make them appear space-like separated when in fact they were not. To remove this possibility, Alice and Bob must agree on a time reference so that they can tell if their signals have been delayed.

Another mode of attack to guard against is for Eve to cause Bob to misjudge the arrival time of the photon from Alice. If Eve found a way to bypass Bob's delay line, she could hold the photon until she had the basis information yet still inject a false signal into Bob's detector that would emulate a photon arriving earlier. Bob can guard against this attack by restricting his collection mode to one that must contain the delay, or physically closing the acceptance aperture (e.g., with an electro-optic switch) after receiving the signal. In that case, if Eve were to attempt delaying the signal, Bob would never receive it. Again, quantum non-demolition measurements (detecting the presence of a photon without measuring or disturbing it's polarization) are presently technologically infeasible, Bob and Alice need to have a pre-agreed time reference so Bob knows when to seal his aperture.

It is often desirable to incorporate a passive-choice element into the sending and/or receiving end of a QKD system. Receiver passive choice is implemented simply by dividing the signal on one or more beam splitters and sending each part so it is analyzed in a different basis. Sender passive choice is typically implemented by using an entangled photon source, such as spontaneous parametric downconversion (SPDC), instead of several laser sources.[7, 21] The SPDC system generates pairs of entangled photons with the property that independently they have random polarization (analysis in any basis gives a 50-50 split), while in coincidence they are perfectly correlated to have, for example, always orthogonal polarizations. One member of the pair is directed to beam splitters, and the path the photon takes determines the analysis basis, thus passively determining the polarization of the twin photon.

The two main advantages of passive choice are simplification by eliminating active-switching circuits and reducing many possibilities for leakage through side channels. For instance, an active switch for the receiver involves applying 1 kV to a Pockels cell in 1 ns. This generates a large amount of RF radiation, as well as acoustical ringing from piezoelectric properties. In the usual QKD protocol (i.e., not delayed-choice) this may leak information to Eve about the basis selection too early, and allow her to always measure in the same

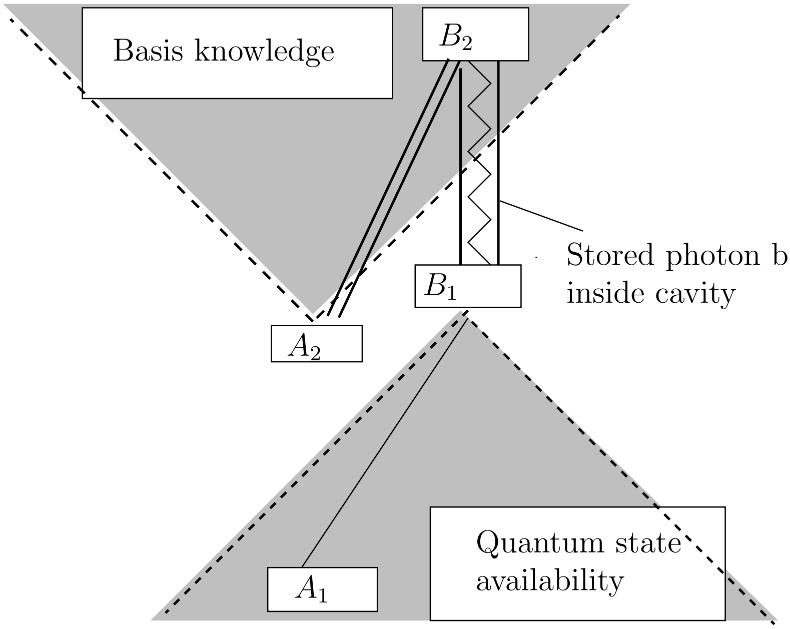
Basis knowledge
B_2
Stored photon bounces inside cavity
B_1
A_2
Quantum state availability
A_1

Figure 7. Spacetime diagram of delayed-choice operation. Alice at coordinate A_1 transmits a quantum signal, received by Bob at B_1 (for generality, we allow this transmission to propagate at a speed less than or equal to c). Later, Alice at A_2 transmits the information of which basis to measure in, which Bob receives at B_2, whereupon he measures the stored state. As long as the past light cone of B_1 does not overlap the future light cone of A_2, there is no point in space-time at which an eavesdropper could have access to both the quantum signal measured by Bob *and* knowledge of the basis chosen by Alice, which are necessary to eavesdrop undetectably. This is a sufficient criteria for security even if in Alice and Bob's rest frame, A_2 is "before" B_1.

basis as Bob. Likewise, if the sender uses separate laser diodes inadvertently operating at slightly different wavelengths, Eve could in principle measure the wavelength without disrupting the polarization, and thereby gain key information without being detected. In the entangled photon system, Alice and Bob can easily check that the polarization states are otherwise indistinguishable by verifying Bell's inequality.[22, 23] The coupling of any other degree of freedom (i.e., frequency) to the photon polarization will destroy the polarization entanglement of the initial state, resulting in an elevated BER and a reduced (or negated) ability to violate Bell's inequality. [†] DCQC does not allow Bob to make a passive basis selection, since he must actually choose the analysis basis after receiving the classical information from Alice. However, the DCQC protocol is fully compatible with entangled photons, so there is no reason that Alice cannot use a passive-choice system for sending the photons, as long as all of the appropriate timing constraints can be met.

In summary, we have proposed a new protocol for quantum cryptography that increases the communication efficiency by delaying Bob's setting of measurement basis until after the classical basis information has been sent to him by Alice. This requires Bob to have the ability to store photons without disrupting their polarization state, and we have implemented a prototype delay line for this purpose. This protocol is interesting because it relies on both quantum mechanics and special relativity to guarantee the secrecy of the exchanged key bits. This suggests to us that other protocols in information science may benefit from similar considerations. For instance, the classical bit-commitment protocol cannot be performed with perfect security in classical *or* quantum information,[24] but can be solved by a protocol based on special relativity.[25]

[†] One further advantage of using entangled pairs for QKD is that, conditional upon detection of one photon, the other output mode is projected into a near Fock state, reducing the multi-photon amplitudes associated with laser sources.

Acknowledgments

This work was supported by the Advanced Research and Development Activity, the DCI postdoctoral program, and the U.S. Army Research Office.

REFERENCES

1. S. Singh, *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography*, Anchor Books, New York, NY, 2000.
2. C. E. Shannon, "A mathematical theory of communication," *Bell System Technical Journal* **27**, pp. 379–423, 623–656, 1948.
3. E. Biham and A. Shamir, "Differential cryptanalysis of DES-like cryptosystems," *Journal of Cryptology* **4**, pp. 3–72, 1991.
4. M. Matsui, "Linear cryptanalysis method for DES cipher," *Proc. Crypto'94* **LNCS 839**, pp. 1–11, 1994.
5. N. Stephenson, *Cryptonomicon*, Avon, 2002.
6. C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proc. of the IEEE Int. Conf. on Computers, Systems, and Signal Processing, Bangalore, India*, *Proc. IEEE*, p. 175, IEEE, New York, 1984.
7. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Rev. Mod. Phys.* **74**, p. 145, 2002.
8. D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera, "Quantum privacy amplification and the security of quantum cryptography over noisy channels," *Phys. Rev. Lett* **77**, p. 2818, 1996.
9. C. H. Bennett, G. Brassard, C. Crépeau, and U. M. Maurer, "Generalized privacy amplification," *IEEE Trans. Inf. Theory* **41**, pp. 1915–1923, 1995.
10. D. Bruss, "Optimal eavesdropping in quantum cryptography with six states," *Phys. Rev. Lett.* **81**, pp. 3018–3021, 1998.
11. H. Bechmann-Pasquinucci and N. Gisin, "Incoherent and coherent eavesdropping in the 6-state protocol of quantum cryptography," *Phys. Rev. A* **59**, p. 4238, 1999.
12. W. K. Wooters and W. H. Zurek, "A single quantum cannot be cloned," *Nature* **299**, p. 802, 1982.
13. M. D. Lukin and A. Imamoglu, "Controlling photons using electromagnetically induced transparency," *Nature* **413**, pp. 273–275, 2001.
14. A. E. Kozhekin, K. Molmer, and E. Polzik, "Quantum memory for light," *Phys. Rev. A* **62**, p. 033809, 2000.
15. D. R. Herriott and H. J. Schulte, "Folded optical delay lines," *Applied Optics* **4**, pp. 883–889, 1965.
16. T. B. Pittman and J. D. Franson, "Cyclical quantum memory for photonic qubits," *Phys. Rev. A* **66**, p. 062302, 2002.
17. A. E. Siegman, *Lasers*, University Science Books, Mill Valley, CA, 1986.
18. D. G. Enzer, P. G. Hadley, R. J. Hughes, C. G. Peterson, and P. G. Kwiat, "Entangled-photon six-state quantum cryptography," *New Journal of Physics* **4**, p. 45.1, 2002.
19. P. W. Shor and J. Preskill, "Simple proof of security of the bb84," *Phys. Rev. Lett.* **85**, pp. 441–444, 2000.
20. H.-K. Lo and H. F. Chau, "Unconditional security of quantum key distribution over arbitrary long distances," *Science* **283**, pp. 2050–2056, 1999.
21. W. Tittel, J. Brendel, H. Zbinden, and N. Gisin, "Quantum cryptography using entangled photons in energy-time Bell states," *Phys. Rev. Lett.* **84**, pp. 4737–4740, 2000.
22. A. K. Ekert, "Quantum cryptography based on Bell's theorem," *Phys. Rev. Lett.* **67**, pp. 661–663, 1991.
23. D. S. Naik, C. G. Peterson, A. G. White, and P. G. Kwiat, "Entangled state quantum cryptography: Eavesdropping on the ekert protocol," *Phys. Rev. Lett.* **84**, p. 4733, 2000.
24. H.-K. Lo and H. Chau, "Is quantum bit commitment really possible," *Phys. Rev. Lett.* **78**, pp. 3410–3413, 1997.
25. A. Kent, "Unconditionally secure bit commitment," *Phys. Rev. Lett.* **83**, pp. 1447–1450, 1999.