6

An Application of Quantum Networks for Secure Video Surveillance

Alan Mink, Lijun Ma, Barry Hershman and Xiao Tang
National Institute of Standards and Technology,
USA

1. Introduction

Security is an increasingly growing concern for network communications and video is an emerging segment of network traffic that uses large amounts of bandwidth. Streaming video, vs. downloading a video for later viewing, requires a continuous, high data rate. The data rate will vary depending on the quality of the video. Video surveillance is a streaming video application that in addition may require securing the data stream to prevent others from viewing it as well as prevent any tampering of that video stream.

There are two parts to secure communication, key distribution and ciphers. A cipher requires a secret key that is used to encrypt data (plaintext), transforming it into an unreadable form (ciphertext) and then to decrypt it back into its original form. Key distribution is the method used to exchange the secret key between the desired end users and no one else. Current block ciphers are relatively slow compared to existing bandwidth because they require a substantial amount of processing that must compete for CPU cycles with the video encoding and compression processing. Frequently changing keys is thought to increase security, but the public key exchange method requires even more processing than the cipher. Cipher and key exchange processing can be off-loaded from the CPU, when the communication end point is the other end of the link, by using dedicated hardware called a link encryptor.

Current classical security algorithms are based on the perceived computational complexity of certain mathematical functions and have not been proved secure. The public key algorithm is at risk from future quantum computers, whereas block ciphers are only weakened and an easy fix is to double the length of the key. Both are constantly at risk from a potential break through algorithm. Communications channels that exploit properties unique to quantum systems have been shown to enable functionality that cannot be achieved by classical means. If a high level of security is deemed necessary for the video stream, one might consider the use of a One-Time-Pad cipher [Wikipedia 2010], the only provably secure cipher, along with Quantum Key Distribution (QKD), also a provably secure method of exchanging the secret keys used by a cipher.

QKD is a protocol based on the quantum laws of physics and is provably information theoretically secure to accomplish key distribution [Gisin, et al., 2002]. QKD keys, when used with a One-Time-Pad cipher, can provide secure communications. A One-Time-Pad cipher algorithm performs an Exclusive OR (XOR) on a random secret key and the message. This is a simple operation that incurs little overhead compared to the more common

computationally intensive ciphers, but it requires the key to be the same length as the message and discarded once used. For video, that requires a continuous stream of random secret keys, which is one of the features of QKD. Because of that feature, QKD is considered to have a long-term security perspective because of its "perfect forward security" attribute. The term perfect forward security means that any compromised keys cannot be used to determine other keys, either past or future. Since QKD keys are random strings and are not produced by a mathematical function, any compromised keys cannot be used to determine other keys.

QKD is still a technology under development even though a few commercial systems are available [Ouellette, 2004]. Some of the limitations of QKD are speed, distance and cost. Distance is a major concern, since without a break-through in developing a quantum repeater the quantum signal is limited to a few 100 km at best. Amplification is not possible since the quantum "no cloning law" specifies that a quantum state cannot be copied. If trusted, intermediate nodes are acceptable, then longer distances are possible via a multi-hop propagation of the key over multiple QKD links. This is not always acceptable and for these situations a quantum repeater would be required. It is currently under development, but none have yet been demonstrated. Speed, the ability to produce secure keys at a high rate is important to cope with the large amount of communication traffic over high-speed connections and hardware implementations that off-load the CPU have been demonstrated. Cost is an ever-present constraint and designs that use lower cost components and share rather than replicate components reduce the cost. In some cases, designs that share rather than duplicate components help to reduce concerns of side channel attacks upon engineered components (vs theoretical ones), but usually at the detriment of speed.

This chapter includes a short summary of the BB84 QKD protocol and its various stages. We then present a section on the configuration of a QKD system targeted for short distances and how a number of innovations lowered the cost and evolved that core design for longer distance communication and current infrastructure use. Another section will discuss hardware support for the data handling necessary to implement high-speed QKD. Extending QKD point-to-point systems to form QKD networks makes it even more attractive for applications such as video surveillance and we will discuss early networking demonstrations. In closing, we will discuss initial QKD standards efforts currently being conducted

2. BB84 protocol

The basic QKD protocol is known as BB84 [Bennet & Brassard, 1984] and has evolved into a family of protocols as researchers experiment with various approaches within a common framework. The BB84 protocol consists of four stages, see Fig 1. The first stage is the transmission of a randomly encoded quantum information stream between Alice (the initiator) and Bob (the responder) through an unsecured public link (called the quantum channel) to establish the raw key. The quantum information stream consists of quantum bits, called "qubits". Photons are used for qbits because light travels well over distances while atoms are better for storage, as in quantum memory, because they are easier to hold in one place. This is the most technically challenging stage of the protocol and has inspired many variations. Horizontal-vertical and diagonal states of photon polarization are a pair of quantum states that cannot be precisely measured simultaneously and are common candidates for QKD. For example, Alice sends each photon set in one of the four linear

polarization states: horizontal-vertical (belonging to the horizontal-vertical basis) or +/- 45 degree diagonal (belonging to the diagonal basis). One of the polarization states in each basis represents a "0" bit value and the other a "1". Alice keeps a temporary database of the state of all photons sent. Bob randomly chooses to measure each photon in either the horizontal-vertical or diagonal basis. Since there is only a single photon, Bob can only do a single measurement. If Bob chooses correctly, the value he measures will be correct. If he chooses incorrectly, the value he measures will be random.

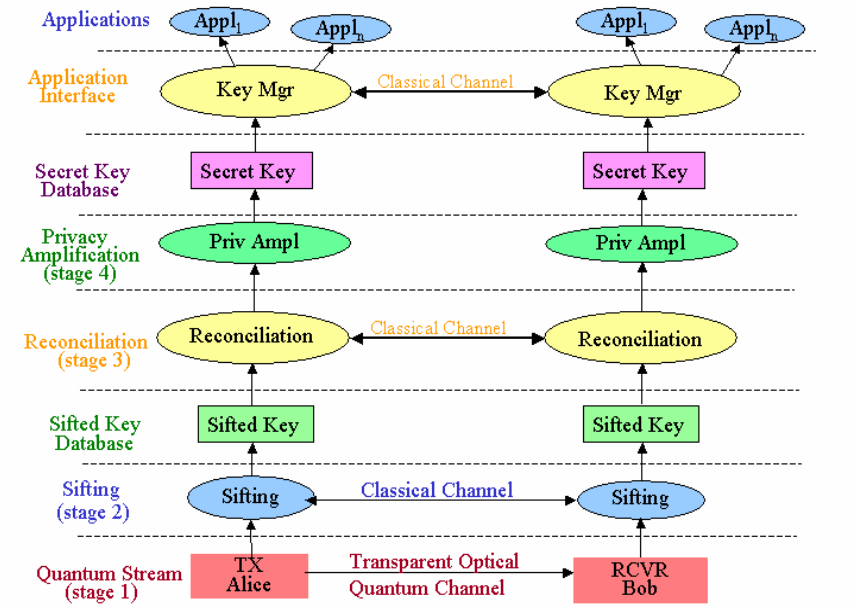


Fig. 1. QKD protocol flow with a Key Manager Application Interface

The remaining stages of the protocol are conducted over an unsecured public link, called the classical channel (this can be any conventional communications channel). The classical channel may be implemented as multiple physical and/or logical channels (e.g., multiple IP sockets for the different protocol stages). The QKD messages sent over them must be authenticated (integrity protected) to prevent tampering, although encryption is not needed since secrecy is unnecessary. The second stage is sifting, where Bob sends a list to Alice of photons detected and how they were measured (basis), but not their measured value. Alice retrieves, from her temporary database, only those entries measured by Bob in the correct basis and sends this list back to Bob (without their values), informing Bob which of his measurements were correct. Bob only keeps those entries on Alice's list. Alice and Bob now have a list of ordered random bits called sifted-keys. These two lists are the same length and, in theory should be identical. However, in practice the lists have some errors between them called quantum bit errors. The quantum bit error rate (QBER) may be caused by ordinary communication noise, but may also be a potential indication of eavesdropping. The eavesdropper is commonly called Eve. If the QBER is low enough, the protocol proceeds to the next stage. If the QBER gets too high the protocol cannot be sure that Eve's information is limited and the current group of sifted-key is discarded.

The third stage is reconciliation to correct these errors. Cascade [Nakassis, et al., 2004], and its variants, is the predominant reconciliation algorithm that exchanges parity and error correcting codes to reconcile errors without exposing the key values. This process requires a number of communications between Bob and Alice and results in a list smaller than the sifted list, since some of the keys are discarded to reduce any information Eve may glean from these exchanges. Niagara [Elliot, et al., 2005] is another algorithm that is based on a low-density parity check method and requires a single exchange between Bob and Alice.
The fourth stage is privacy amplification, which computes a new (even smaller) set of bits from the reconciled set of bits using a hashing algorithm and requires no communication between Alice and Bob. The purpose of privacy amplification is to significantly reduce any information that Eve may have acquired from this protocol. Unless Eve knows all or most of the original bits, she will not be able to compute the new set.
A simplified version of BB84 that reduces complexity, called B92 [Bennett, 1992], uses only two nonorthogonal quantum states, but is considered less secure and is used mostly in R&D to evaluate different QKD implementations and only focuses on stage 1 and 2 of the protocol.
A conventional threat model assumes Eve intercepts the photons, measures them and generates new photons based on those measurements, which are sent to Bob. From this attack, Eve will introduce on average a 25% QBER in the raw key that Bob recovers. Even using other more complex attacks that involve entanglement, Eve still cannot eavesdrop successfully to obtain the keys without introducing a detectable QBER in the raw key. Furthermore, privacy amplification can be strengthened to compensate for these attacks when the QBER is within acceptable bounds. Attacks that focus on side channels and the reality of engineered (vs theoretical) components [Scarani & Kurtsiefer, 2009; Xu, et al., 2010] are a concern for all security measures.

3. A high speed QKD system

We present, as an example, our design of a high speed QKD system. This system was designed for high-speed, short distance communication (< 10 km) and (relatively) low cost. It can operate over a free-space or fiber optic quantum channel. This system uses Vertical-Cavity Surface-Emitting Lasers (VCSELs) for attenuated photon sources, silicon avalanche photo diodes (Si-APDs) for detectors and a pair of custom printed circuit boards (PCBs) [Mink, et al., 2006] to process the QKD protocol data at a continuous high data rate to create a shared sifted-key. A fiber based QKD design is shown in Fig. 2. This system operates the quantum channel at 850 nm and the classical channel in the standard 1550 nm telecommunication range. Both channels operate at the same synchronized 1.25 GHz rate.
Si-APDs are relatively low cost single photon detectors that operate at room temperature in a free running mode with a relatively high quantum efficiency (QE) of about 70% for the optimal wavelength. We chose 850 nm for the quantum channel because it's one of the (older) standard telecommunication wavelengths and thus has commercially available components, even though it's not the optimal wavelength for QE. Also 850 nm is a good short-range wavelength for both free-space and fiber optic transmission. We also chose polarization as the quantum property to encode information on single photons. This is common in QKD. In free-space, the polarization of light doesn't change, although it does in fiber optics and that requires additional handling to compensate for externally caused distortion.

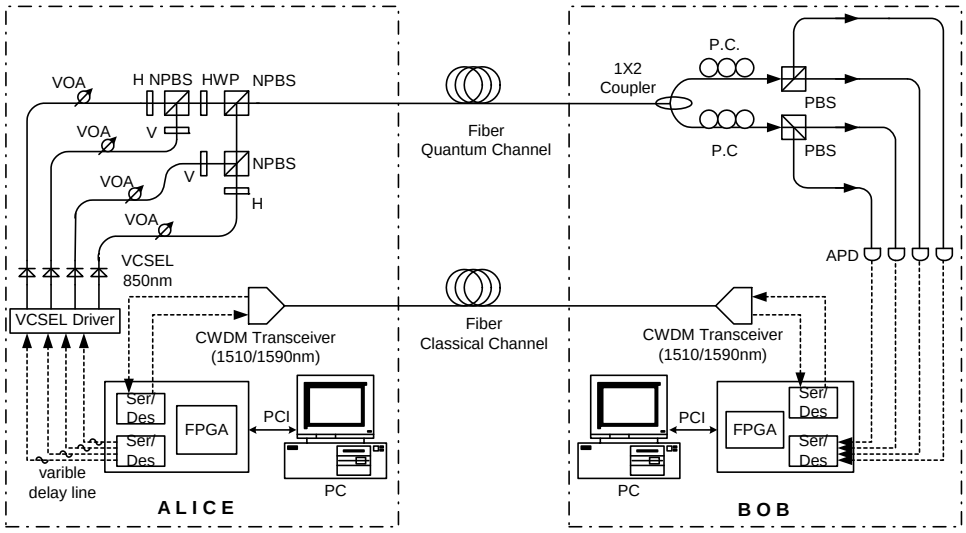


Fig. 2. Schematic diagram of our BB84 fiber-based QKD system; VCSEL: vertical-cavity surface-emitting lasers; Pol.: polarizer; VOA: variable optical attenuator; NPBS, non-polarizing beam splitter; P.C.: polarization controller; FPGA: custom printed circuit board controlled by a field-programmable gate array; PCI: PCI bus; PBS: polarizing beam splitter; Solid line: optical fiber; Dotted line: electric cable

Two commercial 1.25 Gb/s course wavelength division multiplexing transceivers form the bi-directional classical communication channel operating at 1510 nm and 1590 nm. Bob's PCB recovers Alice's clock from the classical channel, allowing it to synchronize with Alice. The clock frequency dictates the resolution of a detection event time bin. Synchronized, aligned time bins are important because the QKD protocol requires Alice and Bob to communicate about specific photons and a way to identify them is by labeling their occurrence in time. The concept is to treat each detector output as a serial data stream and search it for a rising edge (a 0-to-1 transition) indicating a single photon detection event. The bit position in that data stream is the time bin. These time bins can be aligned between Alice and Bob by correlating events in the classical channel to events in the quantum channel.

Alice's PCB generates an 800 ps electrical pulse every 1600 ps (625 MHz) on the randomly selected quantum output. Each of the four outputs drives a 10 Gbit/s 850 nm VCSEL that generates a laser pulse. The intensity of the laser pulse is then attenuated by variable optical attenuators (VOA) to the single photon level. A linear polarizer and a half-wave plate (HWP) sets the polarization orientation, -45^{o}, +45 ^{o}, 0^{o} or 90 ^{o}, that corresponds to the output path. These four output streams are combined into a single stream by non-polarizing beam-splitters (NPBSs) and sent to Bob over the quantum channel. The mean photon number, μ, at Alice's output is set to 0.1, therefore on average, Alice emits one photon every ten pulses.

At Bob, a 1 x 2 non-polarizing single-mode fiber coupler performs a random choice of polarization basis measurement. After the coupler, a polarization compensation module recovers the photon's polarization state and a polarizing beam-splitter (PBS) separates the photons by their polarization directing them to a Si-APD that feeds Bob's PCB. This process separates the photons into four paths, corresponding to the four BB84 encoding states. A photon measured in the wrong basis would be randomly detected as a "0" or "1".

Polarization compensation is needed continuously for a fiber-based system. Initially, and periodically, Bob cooperates with Alice to recover the photon's polarization state that may change during transmission through the fiber. We developed two types of active polarization controllers [Franson and Jacobs, 1995] for a polarization recovery and auto-compensation subsystem [Ma, et al, 2006], since it avoids back-scattering issues of passive polarization controllers [Stucki, et al., 2002]. One type uses liquid crystal retarders (LCR) and the other type uses Piezo Polarization Controllers (PZ), see Fig 3. We chose the PZ controller over the LCR because the PZ is faster (30 μs vs 100 ms), it doesn't need to be aligned with the PBS, it's fiber based with virtually no insertion loss and it can achieve an arbitrary transformation. The disadvantages of the PZ controller are it may drift slowly and it exhibits poor repeatability that results in additional search time.

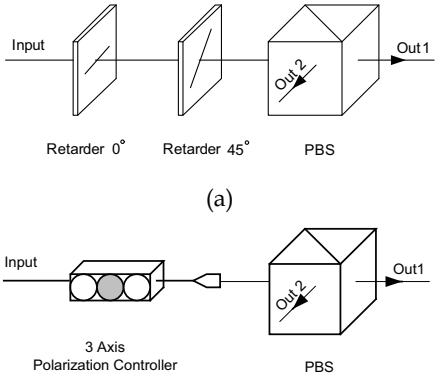


Fig. 3. Two active polarization recovery and auto-compensation (PRAC) subsystem: (a) Liquid Crystal Retardance and (b) Piezo Polarization Controllers.

These controllers maximize the polarization extinction ratio, which is the ratio of the correct photon counts to the incorrect counts in a compatible measurement basis. For example, the ratio between the counts of the two output ports of the PBS when a photon stream of all the same polarization is sent. The algorithm that controls these subsystems does a coarse-step search to find the optimal area and then a fine-step search in that area to find the optimal point. This procedure is run at startup and then invoked periodically or when the QBER increases.

A practical QKD system must be able to use existing fiber infrastructure. We have devised a technique that allows 850 nm single photons to share standard telecom fiber, SMF-28, with telecom traffic. Since the cutoff wavelength of SMF-28 fiber is much longer than 850 nm, some higher order transverse modes (LP_{11} mode) exist in the fiber and travel slightly slower than the fundamental mode (2.3 ns/km delay). Also its polarization state is different than the fundamental mode. At high data rates, when the detection time bin is small this higher order pulse can occur in an adjacent time bin, see Fig. 4(a), and be erroneously detected causing an increase in the QBER. Fusion splicing a short piece of HI780 fiber to the end of the SMF-28 fiber functions as a spatial filter and partially filters the higher order mode pulse [Townsend, 1998; Gordon, et al., 2004], see Fig. 4(b), allowing the 850 nm quantum channel to successfully coexist with 1550 nm traffic on standard telecom fiber.

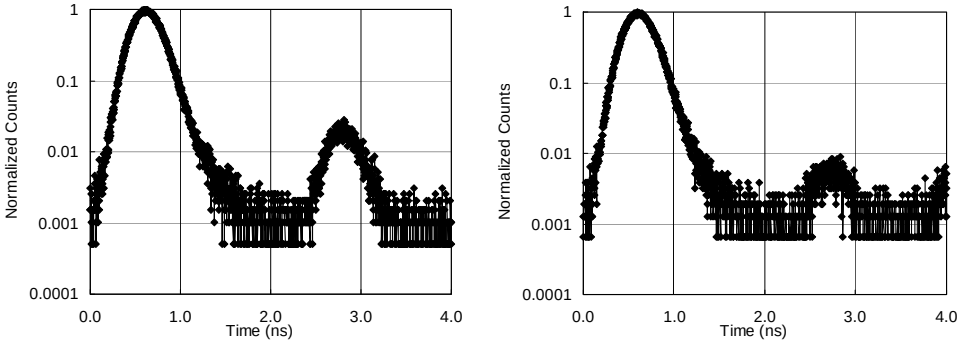


Fig. 4. A photon detection histogram of our 850 nm quantum channel over 1 km of 1550 nm single-mode fiber (SMF28): (a) no splice and (b) ≈40 cm of HI780 fusion-spliced at fiber end.

The quantum channel has a high loss. It is common to only detect a few photons for each 1000 attempts to generate them. Because attenuated sources generate photons based on a Poisson distribution and the intention is to minimize any multi-photon generation, a typical mean photon number, μ, of 0.1 is used. These results in nothing generated ≈89% of the time, one photon generated ≈10% and more than 1 photon generated ≈1%. Thus there is a ≈90% loss right at the source. Normal attenuation applies to the photons in the transmission medium and additional loss is encountered at detectors. In addition to the detector QE, which indicates the percent of photons detected vs. the number that actually arrive, there is also the detector dead time. After an APD detects a photon, the avalanche process generates an electrical output signal. The device then needs a certain amount of time (dead time) to recover to its initial operational state for detection of the next photon. During this dead time, the bias voltage across the p-n junction of the APD is below the breakdown level and no photon can be detected [Ghioni, et al., 2003]. Our Si-APD has a QE of ≈45% at 850 nm, InGaAs APDs (another common QKD detector) tend to have a QE of ≈10% while other types of detectors can have a QE as low as ≈1%.

Two important performance metrics of a QKD system are the secure key generation rate and QBER. Sifted-key rate is related to secure key rate and is a common metric used to evaluate the first two stages of a QKD system. Fig. 5 shows the measured sifted-key rate and the QBER at two quantum transmission rates, 625 Mbit/s and 312.5 Mbit/s, and two fiber lengths, 1 km and 4 km. Demonstrating this system can provide more than 4 Mbit/s of sifted-key over a 1 km of fiber with a mean photon number of 0.1. However, due to the relative high attenuation of 850 nm light in optical fiber, the sifted-key rate decreases quickly (logarithmically linear) as the distance increases, to about 1 Mbit/s at 4 km.

Environmental QBER in our system is mainly caused by the following factors: (1) Si-APD dark count rate and light leakage, (2) cross-talk caused by an imperfect polarization extinction ratio, (3) timing jitter and (4) high order mode noise. Dark counts are caused by a thermo-initiated avalanche process in the APD and unexpected photon detection. They are independent of the transmission rate and for our system are on the order of 200 per second. With proper light sealing and filtering, the counts can be reduced to a few tens per second. Compared to our Mbits/s detection rate, this factor is negligible. The polarization extinction ratio was measured to be between 23 dB to 28 dB, resulting in a contribution of about 1/3 of

the QBER and is independent of the transmission rate. Timing jitter also limits the transmission rate. Timing jitter is mostly caused by the original optical pulse width, its jitter and the timing jitter of the APD. Our optical pulse width is 800 ps (FWHM), and the jitter of the APDs is measured at about 180 ps (FWHM). We also observed APD count-dependent jitter [Gordon, et al., 2005] and VCSEL data-dependent jitter [Guenter & Tatum, 1998] during transmission of randomly encoded photons. Because of this jitter, our detection window is limited to 1.6 ns. Narrowing our detection window results in a higher QBER. High order mode noise contributes about 1/3 of the QBER after filtering. All of these factors yield a QBER for our QKD system of about 2% to 3%. High order mode noise and photon attenuation do slightly increase the QBER at 4 km compared to 1 km.

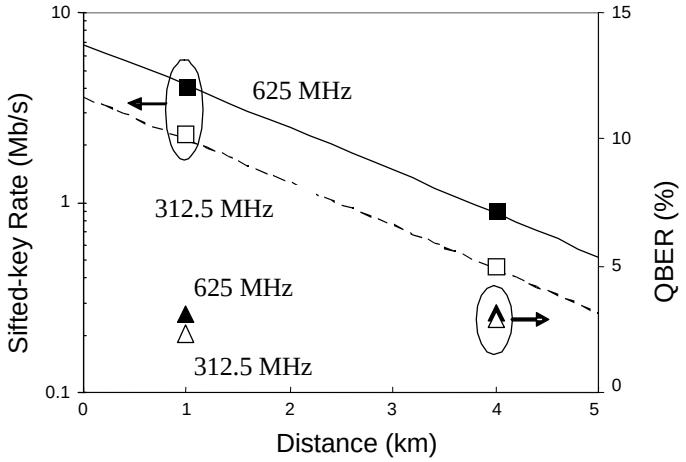


Fig. 5. The system performance of our 850 nm QKD system at 625 MHz and 312.5 MHz.

There are other variations for BB84 implementations that we briefly mention here. "One-way weak coherent pulse" QKD [Gisin , et al., 2002] uses polarization (as we've shown above) or phase encoding of quantum information on single photons sent from Alice to Bob. Plug-and-play QKD [Muller, et al., 1997] is where Bob sends a relatively strong, orthogonally-polarized pair of light pulses to Alice, who modulates their relative phase, attenuates them to single-photon levels, and reflects them back to Bob. The relative phase of the amplitude pulses carries the quantum information to Bob. Using free-space [Bienfang, et al., 2004] as the medium (vs. fiber) eliminates the need for polarization control, but adds the need for the acquisition, pointing, and tracking of the photon path between moving platforms, Alice and Bob. Even stationary buildings are moving due to vibration, wind and thermal expansion but optical communication telescopes exist to handle these problems. Satellites are the ultimate targets. The generation of two or more photons in a pulse used in a quantum link poses an opportunity for information to be obtained by an eavesdropper. On-going work continues to build a source that will generate single photons on demand [Granger, et al., 2004]. Using a source to generate entangled photon pairs [Ling, et al., 2008], one sent to Alice and one to Bob, is another approach that both eliminates multi-photon concerns and the need for a random number generator, since each entangled pair produced is randomly encoded and independent from each other. Currently, generating entangled photon pairs is a relatively slow process. Continuous variable QKD [Fossier, 2009] encodes

small deviations of the phase, amplitude, or polarization of a bright optical pulse. The difficulty is in measuring the received data and determining a state when the variance is comparable with the shot noise limit.

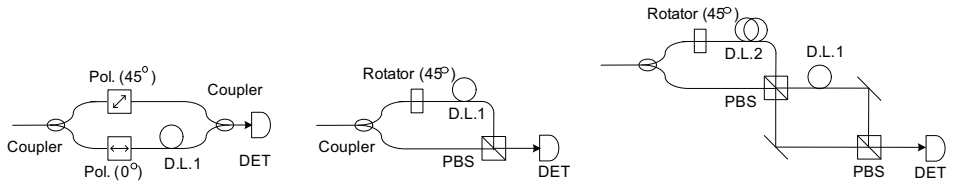
3.1 Reducing the number of detectors

Our high speed 850 nm QKD system uses four Si-APDs, which is the most expensive device in the QKD systems. To reduce the cost and reduce potential side channel attacks of our QKD system, we introduce a detection-time-bin-shift (DTBS) scheme [Breguet, et al., 1994] that projects the measurements into separate time-bins, rather than separate detectors. The disadvantage is the quantum transmission rate is reduced, resulting in proportionately reduced key rates. DTBS schemes can also eliminate side channel concerns caused by self-synchronizing detectors and variations between detector efficiencies. However, when gated mode detectors are used in DTBS schemes, a time-bin-shift (TBS) intercept-resend attack might exploit a side channel and countermeasures should be adopted.

The original DTBS scheme, Fig. 6(a), uses two couplers, each adding a 3 dB loss. In the enhanced scheme, Fig. 6(b), we replace the second coupler with a PBS. A passive coupler performs a random choice of measuring polarization and projects the results onto a short (0° basis) or long (45° basis) delay path resulting in the photon arriving in one of two adjacent time bins. In the short path, the polarization state of the photon is unchanged and is recorded in the first time bin. In the long path, the photon is delayed by one time bin and the polarization state of the photon is rotated by 45° and is recorded in the second time bin. The photons on these two paths are combined using a PBS, thus avoiding a 3 dB loss from a second coupler, and then fed to a single detector. Our scheme of Fig. 6(b) can be further extended to handle all four BB84 states as shown in Fig. 6(c), whereas the original scheme of Fig. 6(a) cannot. By adding another PBS and another pair of paths as well as changing the initial delay to a two time bin delay, we now can map the photon state to one of four time bins. Thus we need to reduce the photon transmission rate by four. The upper path is now a two time bin delay, and thus a photon traversing that path will be detected in time bin two or three, depending on the path it follows in the second pair of paths. The lower path is still a zero time bin delay and thus a photon traversing that path will be detected in time bin zero or one depending on the path it follows in the second pair of paths. Using a DTBS scheme requires only one quantum stream to be aligned to the classical channel, rather than multiple ones. Also during sifting, Bob and Alice must use the transmission clock windows to identify photons, not the DTBS time bins, otherwise the QKD protocol remains unchanged.

Self synchronizing sequences can occur when dead time makes detectors temporarily unavailable, which can result in repeating detector firing order, for example, using two detectors for “0” and “1”, respectively. Once one detector has been fired, it becomes unavailable for the duration of its dead time. In a high photon transmission rate system there is a high probability that the other detector will fire before the first detector recovers. If this sequence of one detector being dead while the other detector fires continues, it results in strings of 1010... . Runs of such strings reduce the randomness of the keys and degrade the security of the QKD system. In our QKD system with 50 ns dead time and a transmission rate of 1.25 GHz, there are 62 (800 ps) time bins for a photon to arrive at the other detector while the first is in its dead time. Because of the quantum channel losses, the 10% emission rate, μ=0.1, of the sources and the QE=45% of the detector, the expected number of photons

arriving in this duration is three. BB84, 4-detector systems suffer from the same problem [Rogers, et al., 2007]. One solution is to disable all detectors once one detector has fired until the dead time has passed and all detectors are available again.



(a) (b) (c)

Fig. 6. Schematic diagram of DTBS schemes: (a) original scheme, (b) enhanced scheme and (c) enhanced scheme for BB84. Coupler: passive fiber coupler; D.L.1: one time-bin delay; D.L.2: two time-bin delay Line; PBS: polarizing beam splitter; DET: single photon detector.

When separate photon detectors are used for different photon values it's difficult to build all photon detectors with identical efficiency. A detector with higher efficiency would fire more frequently than one with lower efficiency. This unbalanced characteristic would cause key values to skew more towards one of the values and undermine the randomness of keys. Using the single detector DTBS scheme of Fig. 6(c), avoids all these problems. Futhermore, some DTBS schemes are also vulnerable to the TBS intercept-resend attack [Xu, et al., 2006] when single photon detectors operate in a gated mode. Some single photon detectors, such as InGaAs APDs, can only work in a gated mode, where photons can only be detected in specified time windows. DTBS systems with single photon detectors operating in free-running mode, such as Si-APD, are not susceptible to this attack.

3.2 Frequency up-conversion for distance

For QKD systems beyond 10 km, the wavelength of the quantum signal needs be in the 1310 nm or 1550 nm bands, where the telecom fiber loss is lowest. WDM and erbium-doped fiber amplifier (EDFA) technology are widely used in current optical communication links and the noise they induce in the 1550 nm band is too high to allow single photon transmission in that band on the same fiber. This leaves the 1310 nm band as a compromise for single photon transmission that can share (WDM) a fiber with existing 1550 telcom traffic.

Among the single photon detectors available for the 1310 nm band, InGaAs APDs [Yuan , et al., 2007], superconducting single-photon detectors (SSPDs) [Hadfield, et al., 2007] and up-conversion detectors using Si-APDs [Langrock, et al., 2005] are used to implement high-speed QKD systems. Recently, a self-difference technique was developed for InGaAs APDs that suppresses the afterpulse noise, and it has been successfully applied to a GHz QKD system [Yuan, et al., 2008]. The InGaAs APD has about 10% detection efficiency, but it still has about 6% afterpulse probability, which would contribute an extra 3% to the QBER of a QKD system. SSPDs can operate in the free-running mode and their response time can be less than 100 ps. However, SSPDs are expensive and need to be operated at 4° K. Si-APDs are low cost, operate at room temperature and have the highest detection efficiency among these detectors, but they don't operate at wavelengths longer than 1000 nm. To alleviate this limitation we implemented an up-conversion detector that transforms 1310 nm single photons into 710 nm photons for detection by Si-APDs.

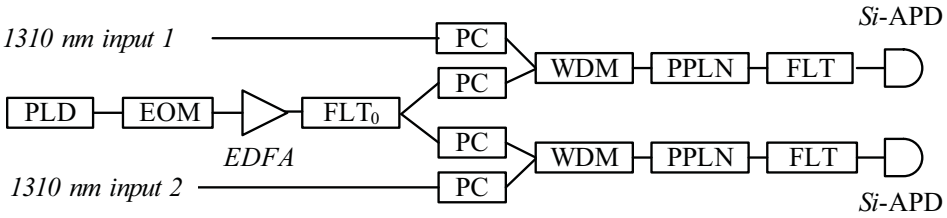


Fig. 7. Configuration of our up-conversion detectors. PLD: laser diode; EOM: Eelectric-optic modulator (LiNbO3); EDFA: erbium-doped fiber amplifier; FLT: optical filter; PC: polarization controller; WDM: wavelength-division multiplexer for 1310 nm and 1550 nm; PPLN: periodically-poled LiNbO3 waveguide module.

Our up-conversion detector [Ma, et al., 2009] structure, based on nonlinear optical sum frequency generation, is shown in Fig. 7. A 1557 nm CW laser diode (PLD) output is modulated to a pulse stream and amplified using an EDFA. A 7 nm (FWHM) optical filter (FLT_0) is used to suppress the EDFA optical noise between 1000 nm and 1300 nm that can induce a large amount of dark counts. After the FLT_0, the 1557 nm pulse is divided into two streams by a 50:50 coupler to function as a pump for two QKD quantum streams at 1306 nm. After polarization control is applied, the 1306 nm QKD signals and the 1557 nm pump are combined by the WDMs and sent to the periodically-poled LiNbO3 (PPLN) waveguide modules where they are up-converted to 710 nm. The output of the PPLN is coupled to a 700 nm single mode fiber, which cuts off the strong 1550 nm pump light, and is passed to the FLT, which contains a 20 nm band-pass filter and a short-wavelength-pass filter, and then finally detected by a Si-APD. This combination of filters helps to attenuate the light between 730 nm to 1000 nm by more than 80 dB. The internal quantum conversion efficiency of the PPLNs is almost 100%, while the overall efficiency of this up-conversion detector is about 20%. The coupling loss is significantly larger than those in [Langrock, et al., 2005] and degrades the overall detection efficiency. PPLN up-conversion is polarization sensitive and can be used as a polarizer, saving a 1 dB loss that a separate polarizer would add.

By using pulsed light at 1557 nm to pump our 1310 nm signal we reduced the noise and the dark counts of our up-conversion detector. The anti-Stokes noise at 1310 is much less than the Stokes noise from a pump whose wavelength is longer than our signal wavelength. Also a pulsed pump can use the same average power as a continuous one while achieving a higher peak power.

The QKD system performance using our up-conversion detector is shown in Fig. 8. During our measurements, the pump power was fixed at 40 mW. The sifted-key rate is 2.5 Mbit/s for a back-to-back connection, 1 Mbit/s at 10 km, and 60 kbit/s at 50 km. The QBER is approximately 3% back-to-back, remains below 4% up to 20 km, and reaches 8% at 50 km. The modulator extinction ratio and system timing jitter induces a background QBER of approximately 2.5% and the rest is from dark counts generated by both the pump light and the classical channel. We set the pump power close to the maximum up-conversion efficiency and the QBER remains small until 20 km due to the low dark count rate of the 1550 nm up-conversion detector.

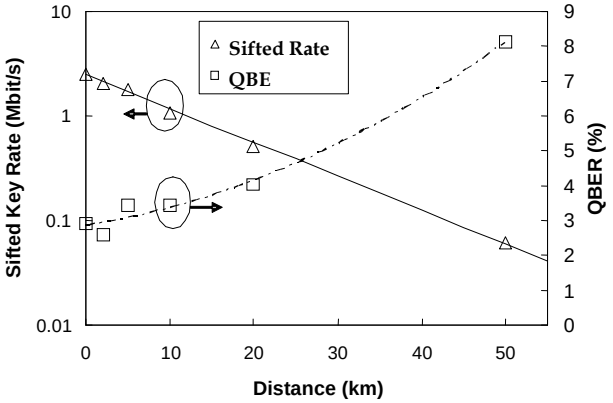


Fig. 8. The performance of our 1310 nm QKD system using up-conversion detectors.

4. Programmable hardware and gigahertz signalling

Because secure video surveillance and other such applications require high speed QKD to generate sufficient secure key, this section will discuss the time tagging, synchronization and data handling necessary to achieve high speed QKD. We focus on an implementation that uses dedicated field programmable gate arrays (FPGAs) and synchronization techniques that enable transmission rates above 1 GHz and avoid some of the data-handling bottlenecks that can limit performance. Research has demonstrated that both the throughput and the signal to noise ratio on the quantum channel of these systems can be improved by operating at high repetition rates and with strong temporal synchronization and gating [Gordon, et al., 2005]. It is well known that the benefits of this approach are ultimately limited by the temporal resolution of the single-photon detectors [Bienfang, et al., 2006]. Available single-photon detector resolution can be below 100 ps (FWHM) [Ghioni, et al., 2007] and can therefore resolve transmission rates well into the gigahertz regime.

For QKD systems operating over kilometer-scale links, synchronization with picosecond accuracy is most commonly achieved with either clock-distribution techniques [Bienfang, et al., 2006], in which synchronization is continuously enforced with active phase-locked-loops (PLLs), or with stable Rubidium oscillators, in which occasional resynchronization processes ensure accurate and synchronous local clocks [Ling, et al., 2008]. The hardware support we discuss in this section focuses on clock-distribution and recovery techniques, mainly because PLL systems are commonly incorporated into commercially available data-processing chips.

With stable synchronization established over the link, detection events can be time tagged by identifying where the detector signal's rising edge occurs with respect to the clock. We view the detector signal as if it were a synchronous serial data stream and implement time tagging by identifying in which bit period the detector signal makes a transition (e.g. 0 to 1). In this approach the serial data rate of the receiver defines the temporal resolution of our time-tagging system; for example, a 1.25 Gb/s serial data rate defines 800 ps time bins. An additional advantage of time tagging with a serial data receiver is that the system operates continuously with no reset time.

Our approach is to use existing chips with transceivers for these tasks to capture serial signals above a GHz and move into the parallel realm for processing at reduced frequencies.

Even at these reduced frequencies, however, feeding the parallel signals into a computer for software processing is not a viable option. Software is a sequential set of operations that requires a certain number of computer-clock cycles for each set of parallel signals. Even with a program designed to operate in the required time period, memory allocations and background applications controlled by the operating system may make it impossible to guarantee that the necessary amount of processing time would be available for continuous signal acquisitions. A 1.25 Gb/s serial signal (800 ps time bins) can be demultiplexed into a synchronous 16 bit parallel word stream at 78.125 MHz. Software that seeks to identify detection events in such a signal would need to execute every 12.8 ns, and complete before the next 12.8 ns time interval. This is challenging even for dedicated real-time computers. A 10 Gb/s signal (100 ps time bins) would generate a synchronous 32 bit parallel signal at 312.5 MHz, leaving only 3.2 ns for processing. And there is the additional difficulty of developing a hardware interface to continuously load the parallel data into the computer at that rate. For such systems, an FPGA board is a flexible approach that can be optimized for a given application and connected to a computer via standard high speed interfaces.

FPGAs can include standard programmable-logic elements, both combinatorial (e.g. AND, OR, NOT) and sequential (e.g. Flip-flop), as well as dedicated specialized devices, such as memory, digital signal processors (DSPs), and high-speed transceivers. FPGAs allow a user to build custom logic sequences that process data acquired from input pins, store the data in internal memory and output the data. Detectors and other devices can be connected directly to FPGA pins and computers can interface with FPGAs using a variety of standard interfaces. FPGA programming is similar to writing a program for a computer, but an FPGA allows the user to control both the data size and operations within each clock cycle, whereas in a computer the operating system and processor make these choices. Controlling the timing sequence becomes an additional "dimension" in programming. Even when the FPGA clock rate is low compared to a given computer, operations can be arranged in parallel and sequenced into tight groups without interruption to compensate for the lower clock rate and achieve comparable or even superior performance.

FPGAs can be programmed to adjust their level of parallelism, but they do not operate at gigahertz rates (yet) and therefore cannot directly process a serial input with sub-nanosecond time bins. Below 1 ns some degree of parallelization is necessary. As discussed above, the faster the input detection stream is sampled by the receiver, the smaller the detection time bins become and the greater the necessary parallelization. Organizing the processing into a pipeline sequence, like an assembly line in which each operation is performed in parallel and a new item can be placed on the assembly line each cycle, allows processing times to exceed the time-bin limit. Current FPGAs can operate with a clock rate up to about 0.5 GHz, though they typically realize only about 1/3 of that rate for all but elementary operations. It is worthwhile to point out that with each new generation of FPGA there has been an increase in operational clock rate of about 10%. Fortunately, data input and output are typically supported at the maximum specified clock rate, and with dual data rate (DDR) capabilities (operating on both the rising and falling clock edges) input and output can operate at speeds up to twice the FPGA's clock rate. By converting a TTL or CMOS signal from a single-photon detector to a differential signal, an FPGA could directly sample the detector signal with resolution down to about 1 ns.

Below 1 ns, front-end circuitry is necessary that will sample the signal and present parallel data to the FPGA at a lower rate. Using existing gigahertz transceivers, or their fundamental core the SerDes (serializer/deserializer), is an attractive choice because they are commonly

available chips and they are included in some FPGAs as internal devices. For input data, a SerDes uses a clock and data recovery (CDR) circuit to sample a serial data stream and recover the clock and data. The SerDes then collects a sequence of the serial bits (in a shift register) and then outputs that group of bits in parallel (to a holding register) along with the recovered clock divided down to the parallel rate. For example, a 1.25 GHz serial input data stream is converted by a SerDes to 10-bit parallel data accompanied by a 125 MHz clock. 125 MHz is much more suited to FPGA processing rates and each parallel data item can be processed in a pipelined manner to maintain a continuous flow of time-tagging data.

One drawback to this approach is that the input serial data stream to a SerDes must be continuous and have sufficient data transitions (balanced) for the internal PLLs to recover the embedded clock. Most single-photon detector signals are random and sparse, with no guaranteed transition interval. For this application, we use additional circuitry to piggyback the single-photon-detector signal onto the known classical channel signal by an exclusive-OR (XOR) before the SerDes as shown in Fig. 9. A similar XOR operation is performed a second time, inside the FPGA, to recover the original detector signal. Thus the balanced classical channel signal provides the timing for the detection stream. It is the rising edge of the detector signal that indicates the arrival time of a photon (the pulse can be given a conveniently long duration provided it does not limit the maximum count rate of the detector). It is the bit period of the classical channel that determines the resolution of the time tags recorded for each single-photon detection event. Finally, time tagging requires a mutual reference event between source and destination that can be used to identify common time bins. This configuration allows such events to be sent over the classical channel, as a predetermined measage.

This approach assumes synchronous signals that are stable when sampled during each clock period. All synchronous electronic devices specify setup (time before the clock edge) and hold (time after the clock edge) times relative to the clock edge when the data must be stable. When the signal is not stable during that period, the output is not deterministic and could result in a metastable [On-Semi, 2007; Unger, 1995; Kleeman & Cantoni, 1987] or undetermined state. This can result in the rising edge being assigned to either of the adjacent time bins somewhat randomly and could add to the overall timing jitter of the system resulting in an increased QBER, and hence fewer usable keys. For this reason the detection time bin should be chosen to be larger than the maximum detector jitter.

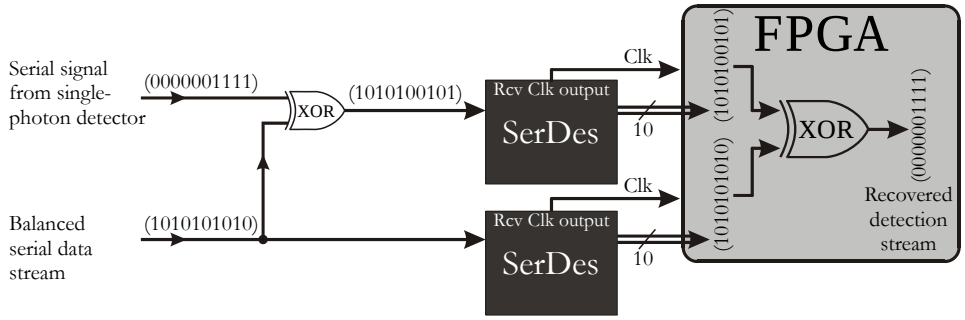


Fig. 9. Piggybacking the sparse signal from a single-photon detector on top of a balanced serial data stream allows the SerDes receiving the single-photon detection events to synchronize to the clock of the balanced data stream. The data and the received clock (Rcv clk) are passed to the FPGA, where the piggybacking signal is removed from the detection signal in a parallel format.

We developed a pair of custom PCB for our GHz-rate QKD system [Mink, et al., 2006], the more complex Bob board shown in Fig. 10. Alice's board is similar, but since its quantum channel is all transmit outputs, it doesn't need the additional front-end receiver logic. To implement the BB84 QKD protocol, we require interfaces for four single-photons detectors. The piggybacking scheme of Fig. 9 is used to sample the detector signal at gigahertz rates and bring it into an FPGA for processing. However, applying Fig. 9 directly results in unstable operation because the jitter in the detector signal can cause transitions at non-regular intervals of the clock. The resulting signal can violate setup and hold times of the SerDes sampling circuit, as discussed above, and potentially cause an unrecoverable metastable condition in the sampling circuit. To avoid this situation we use additional circuitry to stabilize the detector signal, as shown in Fig. 10: two flip-flops (FFs) triggered by the clock recovered from our classical channel. The second FF is necessary because the detector signal can cause instability in the first FF, though it will recover by the next clock edge. We also use two programmable delays: the first aligns the detector signal to the FF clock to minimize the instability in the first FF, the second compensates for the phase difference between the FF output and the clock of the classical stream entering the XOR. Although the clocks driving the FFs are frequency synchronized to the classical stream, they are out of phase due to signal propagation delays on the PCB.

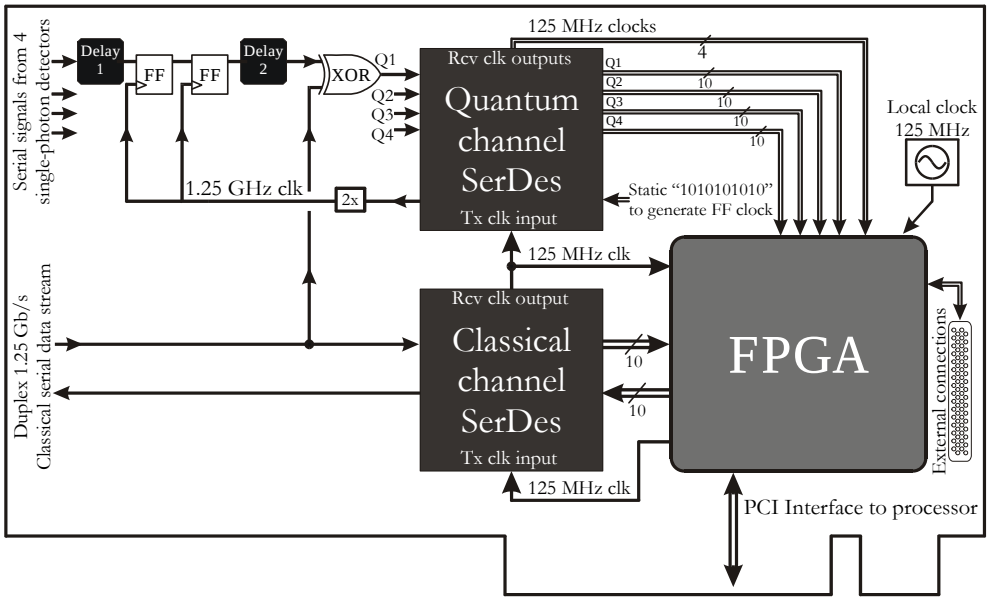


Fig. 10. Schematic of a custom PCB used for QKD experiments. Four single-photon detector channels are recovered using the piggybacking scheme in Fig. 9. Metastability due to detector jitter is avoided with the synchronizing components before the XOR. All four single-photon detector inputs are treated in this manner; only one circuit is illustrated.

The SerDes chip used in this system can support four duplex channels. Each SerDes has one input clock (Tx clk) for all four of its transmit streams, and a separate recovered clock for each receive stream. The two main clocks used by the FPGA are its local clock and the clock recovered from the classical channel. Although these two clocks are nominally 125 MHz,

they are only accurate to within 10^{-4} and are asynchronous to each other. The local clock drives the classical channel transmit stream while the recovered clock from the classical channel is fed to both the FPGA and the quantum channel SerDes. The quantum SerDes uses the classical channel recovered clock to transmit the static 10-bit pattern "1010101010," thus producing a 625 MHz clock. We then double this clock to 1.25 GHz to trigger the FFs synchronously with the classical data stream. Each parallel receive stream from the quantum channel SerDes is fed to the FPGA, along with its own recovered 125 MHz clock, mesochronous to each other and the classical channel. In the FPGA each recovered clock is used to store its associated incoming parallel data stream into dual ported first-in first-outs (FIFOs) that use separate clocks for input and output and can be asynchronous to each other. The FIFOs are capable of synchronizing the data between these two clock domains.

We have built systems using SerDes that are external components connected to the FPGA via PCB traces (c.f. Fig. 10), and more recent implementations [Mink 2007] in which the SerDes are internal to the FPGA package. Internal SerDes saves board space, but in either implementation the interface between the SerDes and the FPGA logic is similar. In most FPGAs the user can configure the operational parameters of internal SerDes. For example, we can change the serial speed of the SerDes to a few predefined points in the range from 1.25 GHz to 6.25 GHz by reprogramming the FPGA.

In addition to timing, the classical channel carries messages to implement the sifting process, where Bob sends its detection events to Alice and Alice returns only the valid ones to Bob. At 1.25 GHz (800 ps detector time-bin resolution) we have achieved a performance of over 4 Mb/s of sifted-key [Tang, et al., 2006], see Fig. 8. Electrical tests have shown the PCBs to have a capacity in excess of 40 Mb/s, though our detectors cannot currently support this rate. This processing reduces the data stream from Gb/s to Mb/s and the resulting sifted-key data stream has no real-time processing constraints; attributes that are attractive for further processing by a computer.

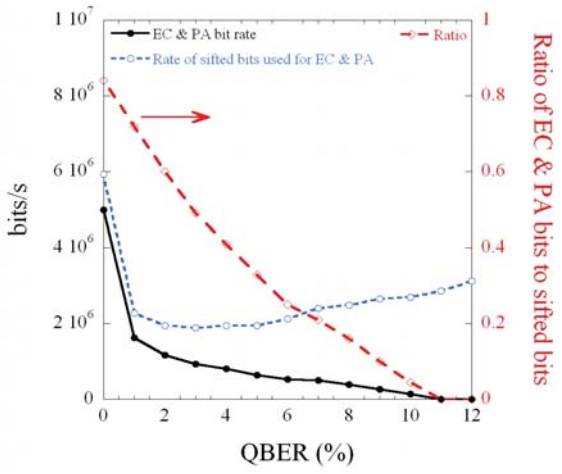


Fig. 11. The maximum processing rate of our EC & PA software implementation (black) as a function of the QBER. For this test the algorithms are running on a typical desktop processor, and sifted bits (blue) are provided as fast as the algorithm can process them (i.e. the output is not limited by the input rate).

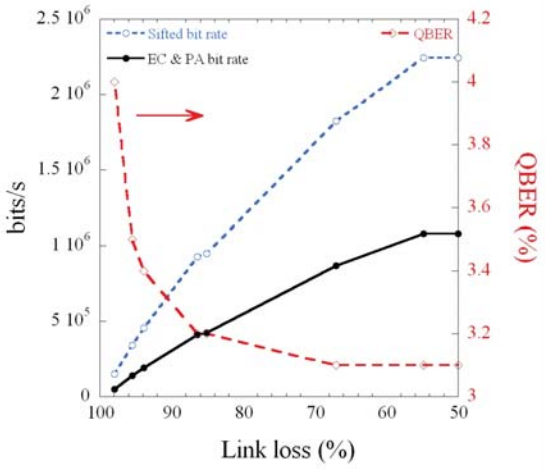


Fig. 12. Performance of our 1.25 GHz free-space QKD system, with the custom PCBs shown in Fig. 10, as a function of link loss. As the optical link losses decrease the high throughput rises until the EC & PA algorithms saturate at about 55% loss.

Once the sifting process has been carried out, subsequent reconciliation and privacy amplification (EC & PA) can be implemented in software or hardware. Reconciliation also requires a classical channel, but it doesn't need to be the same one used by the lower two QKD protocol stages. The processing rate of our software implementation is strongly dependant on computer speed. Fig. 11 shows the maximum output rate of our software EC & PA implementation, as a function of the QBER, when running on a standard desktop system. Our current QKD system can saturate this software implementation. Fig. 12 shows the results from a QKD free-space experiment with a quantum channel transmission rate of 1.25 GHz at 850 nm using Si-APDs. As the link loss is reduced, the sifted-key rate and the EC & PA rates increase and the QBER decreases. At 55% loss and below, rather than continuing to increase, the EC & PA rate reaches a constant value just over 1 Mb/s due to the saturation of our software EC & PA, which in this case is running on a dual-processor machine. The saturation causes the transmit board to wait until space is available before resuming transmission in the quantum channel, resulting in a relatively constant sifted-key rate below 55% link loss. The QBER is not affected. Newer FPGAs now in use are large enough to include our EC & PA algorithms on the chip, but require extensive programming to implement them. The FPGA programming is too extensive to discuss here. On this system, with 1% QBER we have achieved EC & PA secure key rate in excess of 12 Mb/s, significantly greater than the ≈1 Mb/s of our computer software version. To sustain that rate requires a sifted-key rate of ≈15 Mb/s. Our current QKD systems are not able to reach the capacity of this hardware implementation. A further benefit of this hardware implementation is that it removes the significant processing required by the EC & PA algorithms from the CPU and opens those cycles to applications, such as surveillance video.
There are a number of standard high-speed interfaces available for transferring data from an FPGA to a computer. As with FPGA processing one can not expect to achieve the rated throughput; 1/3 to 1/2 of the maximum rated speed is typical. Implementing sifting on the PCB significantly reduces the data rate between PCB and computer, which for us is less than

10 Mb/s. Our QKD board supports a Gb/s PCI interface and a 480 Mb/s USB computer interface. The PCI interface is a 32-bit parallel data interface that runs at 33 MHz. The USB is a high-speed serial interface and an external USB chip on the PCB provides the serial-to-parallel interface and interacts with the FPGA at 33 MHz with 16-bit parallel data. The QKD boards also have an external 65-bit interface (64 data bits plus a clock bit) that allows multi-Gb/s of random number data to be streamed to the FPGA. Operating at 16 MHz, this interface can supply the PCB at a Gb/s. Operating at 160 MHz, this interface can supply the PCB at 10 Gb/s, but at this rate signal integrity may become a concern.
We have found these PCBs to provide a stable and reconfigurable platform for QKD as well as other single-photon experiments. The gigahertz sampling interfaces, the synchronization between source and detector, and the re-programmability of the controlling FPGA, has allowed us to reconfigure these boards for various QKD implementations as well as correlated-photon measurement experiments.

5. Quantum networks and a surveillance video application

Video surveillance usually encompasses more than a single site, but the QKD protocol was designed for a point-to-point implementation. Extending this technology to form quantum (or QKD) networks makes it more attractive to such applications. A QKD network is an embedded sub-network within a conventional communication network for the purpose of developing shared secrets, not transporting secure messages. The secure messages are transported on the conventional communication network. The quantum and classical channels may be dedicated or they can share (via WDM) the existing physical network links of the conventional network, but the quantum channels must have an end-to-end transparent optical path between each QKD node. Building QKD networks and integrating them into conventional networks that support traditional security protocols, and other applications, and use existing network infrastructure is an important step towards the practical deployment of these systems. For deployable systems additional services are required, such as network management and key management with an application interface.
There are two types of QKD networks, passive and active. Passive networks use passive optical components (e.g. the optical coupler) to implement multi-user connectivity. Passive networks can realize multi-terminal communications simultaneously, or "broadcast" from one node to multiple nodes. Several groups have successfully demonstrated a passive QKD network [Phoenix, et al., 1995; Townsend, et al., 1994; Fernandez, et al., 2007]. However, in a passive network, the photons are split by couplers according to their coupling ratio and distributed proportionally to each node, resulting in a proportionally reduced key rate between each node. The second type adopts active optical components, such as optical switches, to dynamically control the communication path. This type is similar to current switched optical communication networks, and establishes a reconfigurable QKD link. Switching time and QKD link initialization are the main overhead factors. Optical switches have been investigated in QKD systems [Toliver, et al., 2003], and demonstrated by BBN Technologies [Elliott, et al., 2005] and NIST [Ma, et al., 2007] but only the NIST system is fast enough to support a one-time pad cipher for video.
A potential solution to extend QKD over longer distances is to chain together a number of QKD links. This approach requires that all intermediate nodes be trusted and secure because the key must be one-time pad transported, in multiple hops, across each additional QKD link to the communication end point, exposing the key at each node. In some cases this may

be acceptable, it depends on the security requirements. For example, this may be acceptable in a corporate application where each node resides within a secure corporate controlled location. This is also applicable to quantum networks where each node cannot be directly connected to each other, such as in a mesh network vs. a star configuration. This also allows the use of non-switched quantum networks where the QKD links are static, such as in the SECOQC network [Peev, et al., 2009]. An example of this multi-hop approach is shown in Fig. 13. There are three QKD links, A-B, C-D and E-F, in a quantum network that connect nodes 1, 2, 3 and 4. QKD link ends B and C are co-located in the same node as are D and E. If we want to send a message from node 1 to node 4, encrypted with QKD key(a), then we need to get key(a) to node 4, but it exists only on Nodes 1 and 2. So node 2 gets key(c) from QKD link C-D and One-Time Pad encrypts key(a) with key(c) and then sends that encrypted key(ac) as a message to node 3. Node 3 decrypts it using key(c), extracting the original key(a). Node 3 then gets key(e) from QKD link E-F and One-Time Pad encrypts key(a) with key(e) and then sends that encrypted key(ae) as a message to node 4. Node 4 decrypts it using key(e), extracting the original key(a).

QKD systems produce a database of ordered secure bits at each end of a QKD link. A key manager, as shown in Fig. 1, is needed to demultiplex and synchronize these QKD bits for various applications, including conventional network security applications such as IPSec and TLS. Demultiplexing divides up the bits in the database into multiple independent key streams for each application. Synchronization makes sure that the same bits, in the same order, are allocated to the same demultiplexed stream on both sides of the network connection. Key management is easier for point-to-point QKD links, but becomes more complex for networks with trusted intermediate nodes since all node combinations must be accommodated. Key management also requires a mechanism to detect and recover from loss of synchronization. The key management application interface, operating within the security perimeter of each local node, would require its peers, as well as applications and their peers, to share a common, unique ID in order to retrieve the proper corresponding key. An application can have as many IDs as desired so it can implement virtual, independent key streams. For example, one for outgoing messages and another for incoming messages.

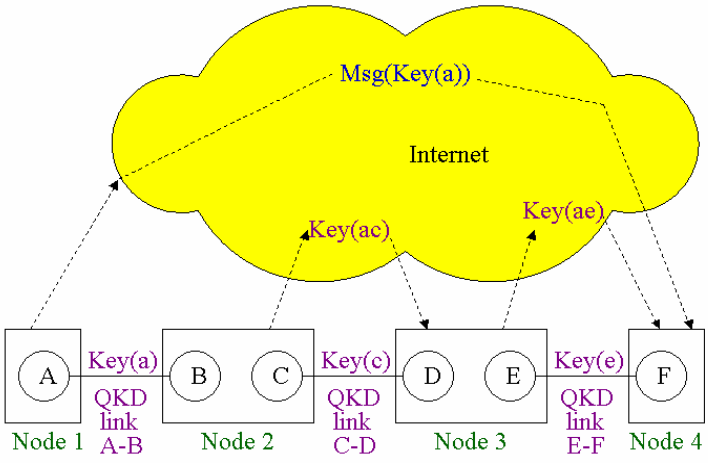


Fig. 13. Example of QKD multi-hop mechanism across 3 QKD links, A-B, C-D, and E-F

Since duplicate secret keys are kept at the respective ends of the channel, there is always a concern that some bits may be dropped or corrupted. A few corrupted bits will ruin a key, but future keys will not be affected. A few dropped bits, however, can be disastrous. Since the keys exist as an ordered set of random bits duplicated at each end of the link, if any bits are dropped at one end and not the other then all future key streams will differ at their respective ends and all future encrypted messages will be undecodeable.

Recovery from a few corrupted bits can be accomplished by discarding that key and obtaining a new key. Preventing such an occurrence can be accomplished by exchanging an error detection hash code for each group of keys transferred at QKD stages. For example, when 1 Mbit of key is transferred from the reconciliation stage to the privacy amplification stage a 64-bit hash code is exchanged to verify their equivalence. If the codes don't match, then that entire group of keys will be discarded. The key manager can take similar actions. At each QKD stage, steps are taken to prevent loss of key synchronization. If high error rates are detected, then the QKD link is reset and restarted. This detects and corrects both corrupted and dropped bits. The secure keys can be labeled by their ordered bit position in the secure key database and the key manager can exchange that information to keep its reserved and multiplexed bit groups synchronized for the applications.

Quantum network management features include controlling the switches, handling routing and verifying that the referenced node does have a currently operational QKD link that can be reached from the current node. Complications arise when switching (vs. static links) is required, because QKD uses circuit switching that requires 10s of seconds to switch, initialize and produce usable keys. Furthermore, periodic adjustments of the quantum channel may be necessary that would cause temporary interruption of the QKD link.

Fig. 14 shows the NIST active, switched quantum network. It has 3 nodes (Alice, Bob1 and Bob2) in a star configuration and uses commercial MEMS optical switches for the quantum and classical channels. The system operates at a 1.25 Gbps clock rate and can provide more than 1 Mb/s sifted-key rate over 1 km of optical fiber. As part of this QKD network, we have developed a quantum network manager and a key manager with an application interface similar to that discussed above. To demonstrate the speed of this QKD system, we have developed a video surveillance application, see Fig. 14, that is secured by a one-time pad cipher using keys generated by this quantum network and transmitted over standard internet IP channels. Two Bobs, at two different locations, are each equipped with a monitoring video camera, and are linked to Alice, who resides at the surveillance monitoring station, through this switched quantum network and the internet. A benefit of a one-time pad cipher is the simple encryption/decryption algorithm that adds little overhead to an application, since it's a bit-by-bit XOR operation of the data stream with the key stream. This, and the QKD hardware support, allows the available CPU cycles to be focused on video surveillance processing and not key and cipher processing.

Our surveillance application uses commercial webcams and an open source media encoder and player, all of which run on standard Windows based PCs. Each webcam output is processed by the media encoder and sends a UDP video data stream to its attached Bob (Linux) machine. Only one Bob (i.e., Bob1 or Bob2) at a time is active and connected to Alice through the switch. Our encryption application, running on the active Bob, receives the video stream as well as a stream of secure keys from its local QKD key manager, see Fig. 1, and performs a one-time pad encryption on the video stream. The now encrypted video stream is sent over the internet to Alice, also a Linux machine. Our decryption application,

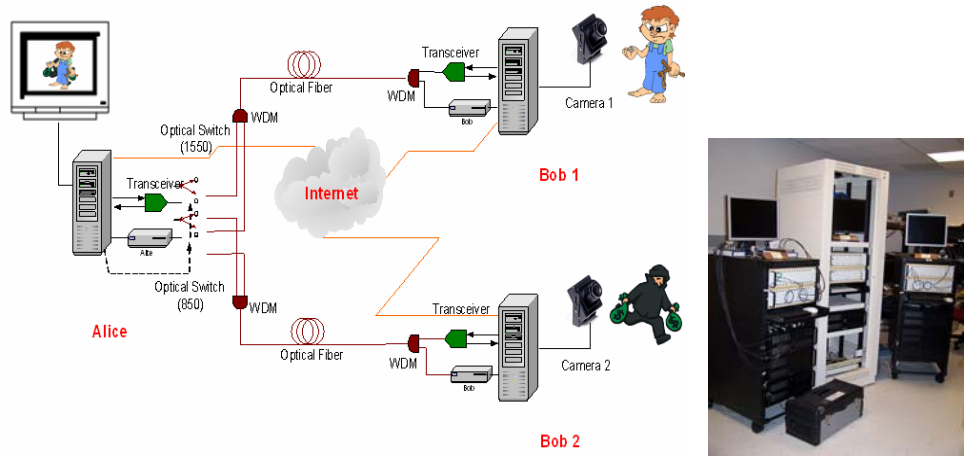


Fig. 14. A Video Surveillance application secured by the NIST QKD network and a one-time pad cipher. Network diagram (left) and actual nodes (right).

running on Alice, receives the encrypted TCP video stream as well as the matching synchronized stream of secure keys from its local QKD key manager. It then uses the key stream to decrypt the video stream and sends the clear text video as a UDP stream to its attached Windows based PC, which is running the media player that displays the video on the PC monitor. The result is continuous video displayed from the webcam, although delayed by a few seconds. Each Windows/Linux machine pair is within a local security perimeter and can be replaced by a single machine by porting the necessary software. When a user at Alice's monitor chooses to switch the video between Bob1 and Bob2, the QKD protocol flow to the active Bob is terminated and his secure key pool is conserved for when we switch back to him. The inactive Bob's QKD protocol flow is started up. The inactive Bob will start to send encrypted video to Alice using any conserved secure keys in its database, otherwise it will stall until its QKD starts to generate keys. An alternative approach to a secure video application would be to integrate the QKD key manager with a conventional network security application, such as IPsec, TLS or a link encryptor. The benefits being a vetted security application and greater portability for the surveillance application.

6. Standards activities

For any significant QKD commercial market penetration, standards are necessary for consumer understanding and verification, and for manufacturers' requirements. Because the QKD community is small, in comparison with the Internet community, only a single initial standards effort could be supported. That effort has been undertaken by the European Technology Standards Institute (ETSI) [Laenger & Lenhart, 2009] with worldwide participation. Delegates come from academia, research centers and industry. The intent of these standards is far reaching. They will need to include definitions and characterization of components (e.g., sources, detectors, random number generators, etc.) as well as the overall system. They will also need to include the metrology necessary to verify component and system operation, and testing to verify conformance to operational and security specifications. Furthermore, standard interfaces are necessary to integrate and interoperate

with existing infrastructure, components and applications. The job is a big one and this standards group is mapping out this complex space. The group was started at the end of 2008 and to complete the underlying work necessary to support these standards and the time to develop the standards will easily take a number of years and will require significant effort from all the member organizations.

7. Conclusion

In this chapter we have discussed the QKD protocol and its potential to secure video surveillance applications. We have shown examples of a QKD implementation along with references to other implementations. We have also shown some innovations that can reduce QKD costs, limit some of the side channel attacks and provide hardware support to off load CPU processing. In addition, we have discussed the expansion of QKD into quantum networks and the concern and complexities associated with trusted intermediate nodes. We also touched on the need for integration with existing network infrastructure, providing services necessary for deployment and an on-going standards effort that is needed by both customers and developers. QKD is an attractive technology that holds significant promise but requires substantial research to bring it to fruition. QKD may not develop into a viable widely deployable technology, but with on-going research at least niche applications have potential.

8. References

Bienfang, J.; Gross, A.; Mink, A.; Hershman, B.; Nakassis, A.; Tang, X.; Lu, R.; Su, D.; Clark, C.; Williams, C.; Hagley, E.; Wen, J. (2004). "Quantum key distribution with 1.25 Gbps clock synchronization", *Optics Express*. Vol. 12, No. 9 (May 2004), pp. 2011–2016
<http://www.antd.nist.gov/pubs/Optics%20Express%20Submiss-1_4_6_04.pdf>

Bennett, C. & Brassard, G. (1984). "Quantum cryptography: Public key distribution and coin tossing", *Proc. of the IEEE Int. Conf. on Computers, Systems & Signal Processing*, pp. 175-179, Bangalore, India, Dec. 1984.
<http://www.cs.ucsb.edu/~chong/290N-W06/BB84.pdf>

Bennett, C. (1992). "Quantum cryptography using any two nonorthogonal states", *Phys. Rev. Lett.*, Vol. 68, No. 21 (May 1992), pp. 3121-3124
<http://prl.aps.org/toc/PRL/v68/i21>

Breguet, J.; Muller, A. & Gisin, N. (1994) "Quantum Cryptography with Polarized Photons in Optical Fibres Experiment and Practical Limits", *J. of Modern Optics*, Vol. 41, No. 12 (Dec. 1994), pp. 2405-2412
http://dx.doi.org/10.1080/09500349414552251

Elliott, C.; Colvin, A.; Pearson, D.; Pikalo, O.; Schlafer, J. & Yeh, H. (2005). "Current status of the DARPA Quantum Network", BBN Technologies, Mar. 2005
<http://arxiv.org/ftp/quant-ph/papers/0503/0503058.pdf>

Fernandez, V.; Collins, R.; Gordon, K.; Paul, P. & Buller, G. (2007). "Passive Optical Network Approach to GigaHertz-Clocked Multiuser Quantum Key Distribution", *J. IEEE J. of Quantum Electronics*, Vol. 43, No. 2 (Feb. 2007), pp. 1-9
<http://arxiv.org/ftp/quant-ph/papers/0612/0612130.pdf>

Fossier, S.; Diamanti, E.; Debuisschert, T.; Villing, A.; Tualle-Brouri, R. & Grangier, P. (2009). "Field test of a continuous-variable quantum key distribution prototype", *New Journal of Physics*,Vol. 11, No. 4 (Apr. 2009), 045023, pp. 1-14 <http://iopscience.iop.org/1367-2630/11/4/045023>

Franson, J. & Jacobs, B. (1995). "Operational system for quantum cryptography", *Electronics Letters*, Vol. 31, No. 3 (Feb. 1995) pp. 232-234 <http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=00362616>

Ghioni, M.; Giudicem, A.; Cova, S. & Zappa, F. (2003). "High-rate quantum key distribution at short wavelength: performance analysis and evaluation of silicon single photon avalanche diodes", *J. of Modern Optics*, Vol. 50, No. 14 (2003), pp. 2251−2269, ISSN**:** 1362-3044 <http://dx.doi.org/10.1080/09500340308234577>

Ghioni, M.; Gulinatti, A.; Rech, I.; Zappa, F. & Cova, S. (2007). "Progress in silicon single-photon avalanche diodes", *IEEE J. of Select Topics in Quantum Electron.,* Vol. 13, No. 4 (July 2007), pp 852-862

Gisin, N.; Ribordy, G.; Tittel, W.; & Zbinden, H.; (2002). "Quantum cryptography", Rev. Mod. Phys. Vol. 74, No. 1 (Jan 2002), pp. 145~195, ISSN 0034-6861 <http://rmp.aps.org/pdf/RMP/v74/i1/p145_1>

Gordon, K.; Fernandez, V.; Townsend, P. & Buller, G. (2004). "A Short Wavelength GigaHertz Clocked Fiber-Optic Quantum Key Distribution System", *IEEE J. of Quantum Electron*, Vol. 40, No. 7 (July 2004), pp. 900-908, ISSN: 0018-9197

Gordon, K.; Fernandez, V.; Buller, G.; Rech, I.; Cova, S. & Townsend, P. (2005). "Quantum key distribution system clocked at 2 GHz", *Opt. Express*, Vol. 13, No. 8, pp. 3015-3020 (Apr. 2005) <http://www.opticsinfobase.org/oe/abstract.cfm?uri=OE-13-8-3015>

Granger, P., et al. (2004). "Focus on Single Photons on Demand", *New Journal of Physics*, Vol. 6, No. 1 (July 2004) <http://iopscience.iop.org/1367-2630/6/1/E04>

Guenter, J. & Tatum, J. (1998). "Modulating VCSELs", *Honeywell Application Sheet*, Honeywell Inc., Feb. 1998 <http://www.imedea.uib.es/~salvador/coms_optiques/addicional/app_notes/honeywell_1.pdf>.

Hadfield, R.; Schlafer, J.; Ma, L.; Mink, A.; Tang, X. & Nam, S. (2007) "Quantum key distribution with high-speed superconducting single-photon detectors", *Proc. of CLEO 07 QML4*, Balt., MD, May 2007 <http://www.antd.nist.gov/pubs/892-papers/High-speed superconducting single photon detectors.pdf>

Kleeman, L & Cantoni, A. (1987). "Metastable behaviour in digital systems", *IEEE Design & Test of Computers,* Vol. 4, No. 6 (Nov. 1987), pp 4-19, ISSN: 0740-7475

Laenger, T. & Lenhart, G. (2009). "Standardization of quantum key distribution and the ETSI standardization initiative ISG-QKD", *New Journal of Physics*, Vol. 11, No. 055051 (May 2009), pp 1-16 <http://iopscience.iop.org/1367-2630/11/5/055051>

Langrock, C.; Diamanti, E.; Roussev, R.; Yamamoto, Y.; Fejer, M. & Takesue, H. (2005). "Highly efficient single-photon detection at communication wavelengths by use of upconversion in reverse-proton-exchanged periodically poled LiNbO3 waveguides", *Opt. Lett.*, Vol. 30, No. 13 (July 2005), pp. 1725-1727 <http://www.opticsinfobase.org/abstract.cfm?URI=ol-30-13-1725>

Ling, A.; Peloso, M.; Marcikic, I.; Scarani, V.; Lamas-Linares, A. & Kurtsiefer, C. (2008). "Experimental quantum key distribution based on a Bell test", *Phys. Rev.* A, Vol. 78 (Aug 2008), 020301 <http://arxiv.org/abs/0805.3629>

Ma, L.; Xu, H. & Tang, X. (2006) "Polarization recovery and auto-compensation in Quantum Key Distribution network", *Proc. of SPIE Optics & Photonics: Quantum Communications and Quantum Imaging IV*, Vol. 6305, 630513, San Diego, CA, Aug. 2006, SPIE <http://w3.antd.nist.gov/pubs/2007/Polarization recovery and auto-compensation.pdf>

Ma, L.; Chang, T.; Mink, A.; Slattery, O.; Hershman, B. & Tang, X. (2007). "Experimental demonstration of an active quantum key distribution network with over Gbps clock synchronization", *IEEE Communications Letters*, Vol. 11, No. 12 (Dec. 2007), pp. 1019 <http://w3.antd.nist.gov/pubs/892-papers/Quantum Key Distribution Network.pdf>

Ma, L; Slattery, O.; Mink, A. & Tang, X. (2009). "Low noise up-conversion single photon detector and its applications in quantum information systems", *Proc. of SPIE: Quantum Communications and Quantum Imaging VII*, Vol. 7465, pp. 74650W, San Diego, CA, Aug. 2009, SPIE
<http://scitation.aip.org/getpdf/servlet/GetPDFServlet?filetype=pdf&id=PSISDG007465000000174650W000001&idtype=cvips&prog=normal>

Mink, A.; Tang, X.; Ma, L.; Nakassis, T.; Hershman, B.; Bienfang, J.; Su, D.; Boisvert, R.; Clark, C. & Williams, C. (2006). "High Speed Quantum Key Distribution System Supports One-Time Pad Encryption of Real-Time Video", *Proc. of SPIE Defense and Security Symposium: Quantum Information and Computation IV*, Vol. 6244, pp. 62440M 1-7, Orlando, Fla., Apr. 2006, SPIE <http://w3.antd.nist.gov/pubs/Mink-SPIE-One-Time-Pad-6244_22.pdf>

Mink, A. (2007). "Custom hardware to eliminate bottlenecks in QKD throughput performance", *Proc. of SPIE Optics East:Quantum Communications Realized*, Vol. 6780, pp. 678014 1-6, Boston, MA, Sept. 2007, SPIE <http://w3.antd.nist.gov/pubs/Next_gen_Paper_5_07.doc>

Muller, A.; Herzog, T.; Huttner, B.; Tittel, W.; Zbinden, H. & Gisin, N. (1997). "Plug & play systems for quantum cryptography", *Applied Physics Letters,* Vol. 70, No. 7 (Feb. 1997), pp. 793–795 <http://www.gap-optique.unige.ch/Publications/PDF/APL00793.pdf>

Nakassis, A.; Bienfang, J. & Williams, C. (2004). "Expeditious reconciliation for practical quantum key distribution", *Proc. of SPIE: Quantum Information and Computation II*,

Vol. 5436, Orlando, FL, Apr. 2004
<http://w3.antd.nist.gov/pubs/orlando.pdf>

Ouellette, J. (2004) "Quantum Key Distribution", *The Industrial Physicist*, Dec 2004, <http://www.aip.org/tip>

ON Semiconductor Corp. (2007). "Metastability and the ECLinPS family", *Application Note AN1504/D*
<http://www.onsemi.com/pub_link/Collateral/AN1504-D.PDF>

Peev, M.; et al. (2009). "The SECOQC quantum key distribution network in Vienna", *New Journal of Physics*, Vol. 11, No. 075001 (July 2009)
<http://iopscience.iop.org/1367-2630/11/7/075001>

Phoenix, S.; Barnett, S.; Townsend, P. & Blow, K. (1995). "Multi-user quantum cryptography on optical networks", *J. of modern optics*, Vol. 42, No. 6 (June 1995), pp. 1155-1163

Rogers, D.; Bienfang, J.; Nakassis, A.; Xu, H. & Clark, C. (2007) "Detector dead-time effects and paralyzability in high-speed quantum key distribution", *New Journal of Physics*, Vol. 9, No. 319 (Sept. 2007), pp 1-13
<http://iopscience.iop.org/1367-2630/9/9/319/pdf/1367-2630_9_9_319.pdf>

Scarani, V. & Kurtsiefer, C. (2009). "The black paper of quantum cryptography: real implementation problems", arXiv:0906.4547v1, quant-ph, June 2009, <http://arxiv.org/abs/0906.4547>

Stucki, D.; Gisin, N.; Guinnard, O.; Ribordy, G. & Zbinden, H. (2002). "Quantum key distribution over 67 km with a plug&play system", *New Journal of Physics* ,Vol. 4, No. 41, (July 2002) pp. 41.1-41.8
<http://iopscience.iop.org/1367-2630/4/1/341>

Tang, X.; Ma, L.; Mink, A.; Nakassis, T.; Xu, H.; Hershman, B.; Bienfang, J.; Su, D.; Boisvert, R.; Clark, C. & Williams, C. (2006) "Quantum key distribution system operating at sifted-key rate over 4 Mbit/s", *Proc. of SPIE: Quantum Information and Computation IV: Proc. SPIE Defense & Security Symposium,* Vol 6244, pp. 62440P 1-8, Orlando, FL, April 2006, SPIE
<http://w3.antd.nist.gov/pubs/Xiao-SPIE-QKD-4mMbps-6244_25.pdf>

Toliver, P.; Runser, R.; Chapuran, T.; Jackel, J.; Banwell, T.; GoodMan, M.; Hughes, R.; Peterson, C.; Derkacs, D.; Nordholt, J.; Mercer, L.; McNown, S.; Goldman, A. & Blake, J. (2003). "Experimental investigation of quantum key distribution through transparent optical switch elements", *IEEE Photon. Technol. Lett.*, Vol. 15, No. 11 (Nov. 2003), pp. 1669-1671

Townsend, P.; Phonenix, S.; Blow, K. & Barnett, S. (1994). "Design of quantum cryptography systems for passive optical networks", *IEEE Electronics Letters*, Vol. 30, No. 22 (Oct. 1994), pp. 1875-1877

Townsend, P. (1998). "Experimental investigation of the performance limits for first telecommunication-window quantum cryptography system", *IEEE Photon. Technol. Lett.* , Vol. 10, No. 7 (July 1998), pp. 1048-1050, ISSN: 1041-1135

Unger, S. (1995). "Hazards, critical races, and metastability", *IEEE Trans. on Computers,* Vol. 44, No. 6 (June 1995), pp 754-768

Wikipedia. (2010). http://en.wikipedia.org/wiki/One-time_pad, last modified July 2010, last accessed July 2010

Xu, F.; Qi B. & Lo H. (2010). "Experimental demonstration of phase-remapping attack in a practical quantum key distribution system", arXiv:1005.2376v1 [quant-ph] May 2010, < http://arxiv.org/abs/1005.2376>

Xu, H.; Ma, L.; Bienfang, J. & Tang, X. (2006) "Influence of the dead time of avalanche photodiode on high-speed quantum-key distribution system", *Proc. of CLEO/QELS Photonic Applications Systems Technologies*, Technical Digest (CD) paper: JTuH3, Long Beach, CA, May 2006, Optical Society of America <http://www.opticsinfobase.org/abstract.cfm?URI=QELS-2006-JTuH3>

Yuan Z.; Kardynal, B.; Sharpe, A. & Shields, A. (2007). "High speed single photon detection in the near infrared", *Applied Physics Letters*, Vol. 91, No. 4, #041114 (July 2007) <http://arxiv.org/PS_cache/arxiv/pdf/0707/0707.4307v1.pdf>

Yuan, Z.; Dixon, A.; Dynes, J.; Sharpe, A. & Shields, A. (2008). " Gigahertz quantum key distribution with InGaAs avalanche photodiodes", *Applied Physics Letters*, Vol. 92, No. 20, #201104 (May 2008) <http://arxiv.org/PS_cache/arxiv/pdf/0805/0805.3414v1.pdf>