Quantum Information Processing, Vol. 1, Nos. 1/2, April 2002 (© 2002)

Another Alternative to Quantum Cryptography

Willard Wells,[1] Jim Menders,[1] Ed Miles,[1] Boris Loginov,[1] and Henri Hodara[1]

Received February 1, 2002; accepted May 3, 2002

Quantum cryptography has several unorthodox attributes: it is invulnerable to passive eavesdropping; communicators need no initial shared secret (cryptographic key), but they do need an auxiliary tamper-proof link; the scheme requires an uninterrupted light path (no repeater), and a one-time pad of keystream must be prepared in advance of the secure transmission. At least two other cryptologic schemes share these same attributes. This is quite remarkable because each of the three schemes has an entirely different physical basis for its message secrecy. In quantum cryptography an eavesdropper cannot measure or clone the state of a photon without revealing the attempt to the authorized receiver. The second scheme is the Yuen–Kim protocol. Potential bits for the keystream are masked by classical noise. The eavesdropper cannot extract the same useful bits that the authorized receiver extracts because their receivers are statistically independent. Our own scheme, called QDRN, distributes broadband noisy light to terminals, where interferometers provide identical keystreams. Security presumes that there exists some bandwidth broad enough so that the eavesdropper cannot store the phase information either optically or digitally for some period like minutes, or even hours if necessary, after which the users may safely transmit data. The Yuen–Kim protocol is by far the simplest to implement. However, it is limited to point-to-point links and distances of some tens of kilometers. By contrast, QDRN operates with full power, is compatible with amplifiers and networks, and extends to hundreds of kilometers, quite possibly a megameter.

KEY WORDS: quantum cryptography; key distribution; cryptology; secure optical communication.

PACS: 03.67.Dd.

INTRODUCTION

We compare three schemes for secure optical communication that share several curious attributes. The first is Quantum Cryptography,[1, 2] AKA,

[1] IPITEK, Carlsbad, California.

1570-0755/02/0400-0091/0

Quantum Key Distribution (QKD). The transmitter, Alice, sends a single photon for each bit of information. She represents the binary ONE and ZERO by two non-orthogonal quantum states. By attempting to measure the states of each photon, the eavesdropper, Eve, perturbs it in a way that betrays her activity to the authorized receiver, Bob.

The second scheme is the Yuen–Kim Protocol (YKP),[3, 4] which has ultimate simplicity. Alice sends Bob a raw one-time pad (1TP) on an insecure channel, but at such low power that his SNR$\ll$1 due to normal Gaussian noise in his receiver. Bob accepts as valid bits only pulses that fall in the two extreme tails of the Gaussian distribution, the ZERO tail and the ONE tail. The idea is that the two extremes occur mostly when the noise and signal add coherently with the same sign (by chance), and since Bob only needs the sign for his binary data, these are the bits he accepts. Bob tells Alice on a public link which bits he is using, but not their value, and these bits comprise a sifted 1TP. Finally Bob and Alice distill this pad by error-correcting techniques and privacy amplification to obtain the reconciled 1TP. Eve is thwarted because her noise is statistically independent from Bob's, and so her choice of valid bits rarely agrees with Bob's. This scheme works (both theory and experiment) even when Bob's SNR is weaker than Eve's by 9 dB. For example, she may be closer to the transmitter by that amount. If fiber attenuation is 0.2 dB/km, this makes the maximum range about 45 km.

The third scheme called QDRN (pronounced kew-darn) is our own invention, which we describe in this paper. Alice sends Bob a broadband lightwave. They both use imbalanced interferometers to convert phase noise into intensity noise. Then they time sample the photodetected noise to obtain 1TPs. An initial protocol ensures that they and they alone agree on the interferometer's settings so that the two 1TPs will be identical within some tolerable bit error rate (BER). Of the three schemes, QDRN is the only one compatible with networks. The other two are inherently point-to-point links because they cannot tolerate the power losses at network junctions. QDRN is also the only one capable of full power and long range, something like 500 to 1000 km. Moreover, a single broadband lightwave can supply the needs of a big facility that loads many 1TPs by using separate interferometers in parallel, but only the one lightwave.

The three security concepts are radically different. Quantum cryptography (QC) depends on the impossibility of measuring or cloning the quantum state of a single photon. YKP relies on Bob and Eve seeing statistically independent noise in their receivers. QDRN relies on Alice's and Bob's ability to use light of such wide bandwidth that Eve cannot store—either optically or digitally—the phase information with sufficient accuracy and for sufficient duration to breach the security of the system. (If advanced

technology ever allows a recording of a broadband wave, then it will surely allow QDRN to increase its bandwidth. The defense will always win this technology race.)

Despite these radical differences, the three schemes share a remarkable number of curious attributes:

1. All three are invulnerable to a passive eavesdropper who merely taps the line and listens.
2. Alice and Bob can set up their session without the aid of an initial shared secret (such as a key from a key distribution center).

However, there is a price:

3. With one possible exception, all three schemes require an uninterrupted light path between terminals—no repeaters.
4. They require a two-way auxiliary link that is not necessarily private, but is otherwise tamper-proof (uninterruptible).
5. The keystream cannot be used in real time. It must be processed to remove intrinsic errors and then stored as a one-time pad.

In view of this impressive list, we wonder if some undiscovered theorem links all five of these attributes, something involving information theory, physics, and/or game theory (authorized users versus eavesdropper). The most obvious linkage is Items 2 and 4. If Alice and Bob share no initial secret, and have no tamper-proof link, then there is no way either one can be sure with whom they are communicating.

None of these three schemes offers absolute message privacy. What they all really do is change the game: Eve attacks the auxiliary link that ensures authenticity. If she succeeds, she severs all links (opaque attack), and installs her own repeaters. Then she impersonates Alice on her link to Bob, and Bob on her link to Alice. (The two 1TPs are different.) The problem of privacy (Item 1 in list) has been converted to a problem of authenticity (Item 4), which may be more readily solvable in many circumstances.

In the following sections, we first describe QDRN, the least familiar of the three schemes. The next section describes our experimental demonstration. The third and fourth sections discuss the use of QDRN in networks and long distance transmission. Two sections give some summary remarks on QC and YKP, and finally we summarize conclusions.

HOW QDRN WORKS

Optical fibers are a natural medium for wideband transmission, a fact that suggests the use of spread-spectrum techniques for secure commu-

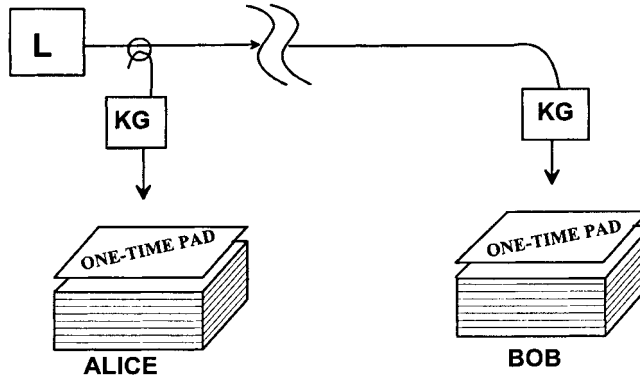

Fig. 1. Key generators based on broadband lightwave.

nications, as in Coherence Tracking[5] for example. QDRN is another scheme in this class, and most likely an improved concept.[6, 7]

A broadband source sends a lightwave to both Alice and Bob (Fig. 1). They use identical key generators that operate on the lightwave to develop identical keystreams, which they load into their respective one-time pads. Figure 2 shows the key generator. Phase noise in the light is the source of our 1TP. An interferometer converts its phase jitter to intensity noise. Detectors measure random power fluctuations, which are filtered to produce an analog keystream. Samples at regular intervals produce a digital keystream, which ideally would be identical at each terminal. The length of the variable delay line is the session key. Figure 2 shows a variable delay line in one arm of the imbalanced interferometer. One obtains a new key by

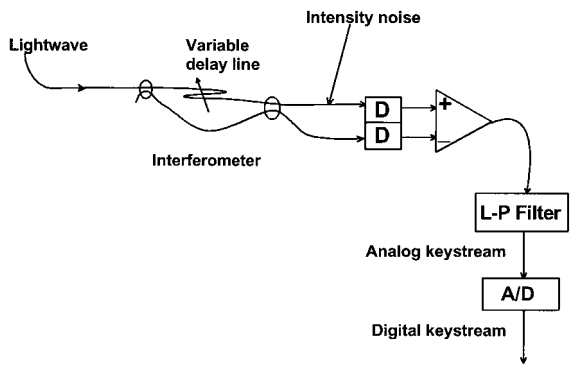

Fig. 2. Key generator.

changing this delay in increments of one coherence length, 3 mm in our case. A change of a half wavelength also produces a new key.

For simplicity Fig. 2 shows only one delay line. To enlarge key space arbitrarily, one can add more components that reshape the analog keystream. The possibilities include a compound interferometer with more delay lines and/or electrical components that alter the analog keystream. All such components have adjustable parameters that add new dimensions to key space.

In common with QC, it is possible to develop a QDRN session key without an initial shared secret. To do this, Bob chooses a key at random, i.e., a length for the delay line in Fig. 2. Alice then scans her corresponding delay line in some random sequence, all the while sending Bob both the lightwave and the keystream in a numbered sequence. When Bob gets a sample of keystream that correlates with his, he knows that Alice has hit on his chosen key. He then tells Alice the sample number by way of the public auxiliary link. She looks at her test sequence and knows the key length for that interferometer. Eve also intercepts the sample number, but it is useless to her since she doesn't know Alice's random sequence of key trials (nor does Bob or anyone else). Alice and Bob repeat the procedure for any other delay lines and variable components until the session key is complete. If the various key dimensions have lengths K, L, M, N, then the scan time for key transmission is proportional to the sum $K + L + M + N$, while key space is proportional to the product $K \cdot L \cdot M \cdot N$. Examples appear in the subsection entitled 'QDRN Key Space' below.

A system with a finite key space is normally vulnerable to exhaustive search. Eve simply tries keys one after another as quickly as possible until she finds the one that produces intelligible data. But in our case Eve cannot know when she finds this prize! Her only way to test a key is to try it on the ciphertext, but the ciphertext is not on line yet and won't be for some minutes, hours, or days. And when it does appear on line, the lightwave that Eve needs to generate the keystream will be long gone, since it is not recordable.

To defeat the system by a key search, Eve needs to preserve the lightwave so she can test interferometer keys later when the users send data. She can try to keep the physical wave and feed it into real interferometers, or she can digitize the wave and feed it into a virtual interferometer by numerical simulation.

Optical. Lightwaves can be preserved indefinitely in a re-entrant large spool of fiber, but not without distortion. Suppose 1000 sec = 17 minutes elapse between transmission of the phase-noise lightwave and transmission of data that which Eve can use to test keys. During that time, light propagates 200 Gm. This is 200,000 times a distance at which distor-

tion becomes noticeable, about 1 Mm. Clearly the wave is useless by then.

Digital. Eve can mix the phase-noise lightwave with the light from one or more local oscillators to get an intermediate frequency (IF), which she then records. We like to use an optical bandwidth of 100 GHz because this is about the maximum we can squeeze into a WDM channel. And so this is the rate that Eve has to record. It takes at least 10 bits to characterize each cycle, so that brings her recording bandwidth to 1 terabit/sec. We typically generate digital keystream at the rate of 10 Mb/sec. To fill a modest buffer, say 10 Gb with raw pad then takes 1000 sec = 17 min. During this time Eve would collect 1015 bits = 1 petabit. If she settles for only 10% of them, it is still 100 Tbits. And storing them is only the beginning of her troubles. She still has to number-crunch them in her supercomputer to simulate the interferometer and thereby find its key.

QDRN requires some means for correcting errors that are inherent to the system. They occur at the A/D conversion in the key generator, Fig. 2. The bit decision, ONE or ZERO, occurs where the analog keystream is compared to a decision threshold. When it's a close call, Alice's key generator will sometimes say ONE when Bob's says ZERO, and vice versa. In a long link, these bit errors occur frequently due to distortions of the lightwave, mainly residual dispersion in the fiber and additive noise from amplifiers. These issues are treated in the section "QDRN and Long Distance Transmission" below, which shows that distances in the range 500 to 1000 km are feasible.

To avoid these errors, each key generator needs three decision levels separated by two thresholds as shown in Fig. 3. The levels represent ZERO, Inconclusive (INC), and ONE. In practice we also base the INC decision on two sample times to allow for timing errors. In other words, an acceptable

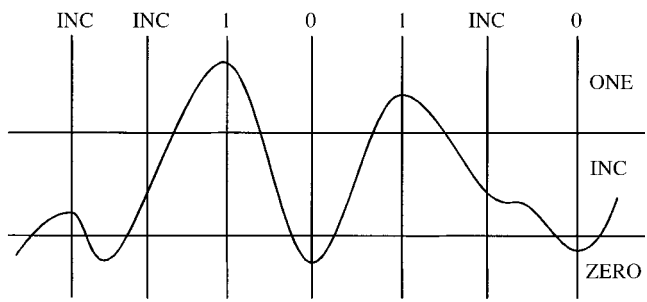

Fig. 3. Dual threshold A/D.

sample must fall outside a little box in the two dimensions of time and amplitude.

Along with the transmission of a raw one-time pad, Alice and Bob communicate over a public link and tell one another which bits are INC. They both erase those from their one-time pads and compact the valid bits to close the gaps. Again this is like QC (see "Remarks on Quantum Cryptography" below): both schemes produce a raw pad with contamination, which then must be distilled to produce the good one.

In summary, the QDRN protocol goes like this:

- Session request: scan interferometers to send the session key.
- Send phase-noise lightwave and store the resulting raw 1TP.
- Wait a time to ensure that Eve cannot maintain the lightwave.
- Transmit bit-validity data—which bits are rejected as inconclusive.
- Compact the sifted key. Do any necessary error correction and privacy amplification to obtain a reconciled 1TP.
- Encrypt the plaintext; send cyphertext.

Operationally, all except the last step may be performed automatically after midnight so that a full backlog of 1TP is ready in the morning.

QDRN KEY SPACE

A vault approved for storage of classified information has a combination with three numbers, each with a hundred possible values (0 to 99), and so the key space is $100^3 =$ one million. By contract, cryptographic engines have key spaces exceeding 10^{17}, the number of possible initial states of the key generator. So why is there a discrepancy of a factor of 100 billion or more? And which of these examples is the appropriate paradigm for QDRN?

The only reason that cryptologic key space is so enormous is that Eve has everything she needs inside her supercomputer: cyphertexts for sure, statistical properties of plaintext that enable her to recognize it, possibly a plaintext that matches one of the cyphertexts, possibly two different encryptions for the same message, and possibly a purchased or stolen copy of the encryption algorithm.

In QDRN this is not the case: Eve lacks the essential copy of the phase-noise lightwave. And so the security issue is more like a combination lock. If an intruder sneaks past IPITEK's staff meeting and reaches the vault, then he might try six combinations per minute for ninety minutes, about 500 trials in all. By comparison, when Eve attacks QDRN, she gets only one shot at the key per receiver that she installs operating in parallel,

each with its own storage for 1TP. Surely she would have fewer than one hundred of these units. And so it might seem that a key space of 10^5 is minimally adequate, but one would probably use much more because it doesn't cost that much. Two examples follow.

Minimal Key Space. Each interferometer in tandem contributes one dimension of key space. Its size is the range of variation in its path length divided by the coherence length L of the phase-noise lightwave, about 3 millimeters in our system. We get another factor of two from the two phases, say 0 and π, set by a phase-lock device. Electro-optic switches put loops of fiber into or out of the path, and these loops have binary multiples of the coherence length, i.e., L, 2L, 4L.... The insertion losses of many switches are a problem, but one we expect the telecommunications industry to solve, because they have a big stake in optical switching.

Suppose we try to get by with a single interferometer. Assume seventeen switches. The number of keys is then 2^{17} or 131,072, times two for phases is about 262,000. The total amount of fiber in the variable range is 131,071 times 3 mm, or about 400 m.

In estimating key agility, the main delay is clearing light out of the interferometer. To clear out 400 m at a velocity of 200 meters per microsecond takes two microseconds. The time to change keys may come to three microseconds, allowing for other delays. The time to scan through all 262,000 keys is then 800 msec, almost 1 second.

Maximal Key Space. Assume two interferometers in series (four light paths) as in Fig. 4. With series interferometers, a small problem arises in how to phase lock the two independently, that is, to derive two control signals from one electrical output. The way we have done this in the past[5] is to dither the lengths of each one at different frequencies. Then each interferometer has its own frequency signature in the electric output. There may be other techniques using dichroic elements to treat the two parts independently.

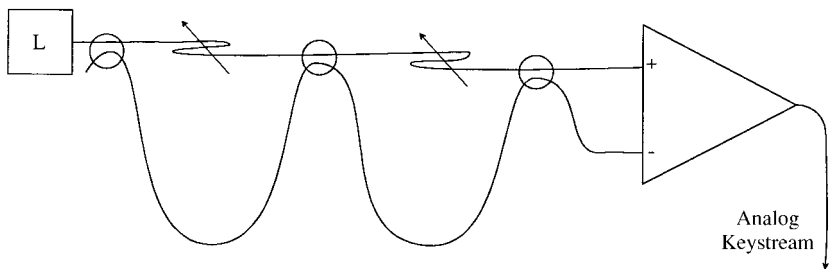

Fig. 4. Interferometers in series.

Let us try thirteen switches in each one for 2^{13}, or 8192 keys, times two for phase, is 16,384 in each of the two keyspace dimensions, which comes to 268 million keys in all. The total fiber in each is $(2^{14}-1)\cdot 3\,\text{mm} = 49\,\text{m}$, say 50 m. For both interferometers, this comes to 100 m. Time to clear out the light is 0.5 μsec. With other delays such as switching, allow about 2 μsec. To transfer the key from Bob to Alice, we disable each interferometer while scanning the other. The time for each is then 2 μs·8200 keys, or 16.4 ms, which comes to 33 ms for both.

QDRN KEYSTREAM DEMONSTRATION

We have built and are integrating a pair of terminals comprising a one-way secure optical link using interferometric key generation. Each terminal is controlled by a PC that also originates or receives test data. We have provided an Ethernet link between the PCs, which we use to send the test data for bit error rate. The system uses three WDM optical channels to transmit the phase-noise lightwave at 1550 nm, data at 1310 and a stable laser phase reference for interferometer stabilization at 1530 nm. An alternative to the reference laser transmission would be to give both Bob and Alice a wavelength standard, probably a laser frequency-locked to an atomic spectral line.

The data channel is also used to identify key bits with an INC value, by associating each key bit of the keystream with a validity bit. At this time, we have succeeded in generating raw keystreams at the transmitter and receiver terminals at a rate of about 10 Mbps, yielding sifted keys, with INC bits removed, at a somewhat slower rate. The Ethernet link between the terminals was used to assess the quality of the binary key generation.

In addition to matching the interferometer's path length differences to much better than the coherence length of the noise lightwave, it is also necessary to match their difference modulo 2π. This wavelength-scale pathlength-matching requirement is met by multiplexing a very coherent signal along with the phase-noise lightwave, and using a servo-loop to lock the asymmetry to, say, a dark fringe at the interferometer's output. We use a fiber stretcher to make wavelength-scale adjustments to the pathlength imbalance of each interferometer. The stretcher is controlled by a servo-loop that seeks to null the transmission of the probe beam.

To demonstrate key generation, we used a single interferometer to generate the intensity noise as in Fig. 2. The terminals converted the intensity noise to electronic noise independently. In its present stage of development, we have demonstrated the acquisition of identical keystrings (from raw keystrings) at both the transmitter and receiver terminals. Figure 5

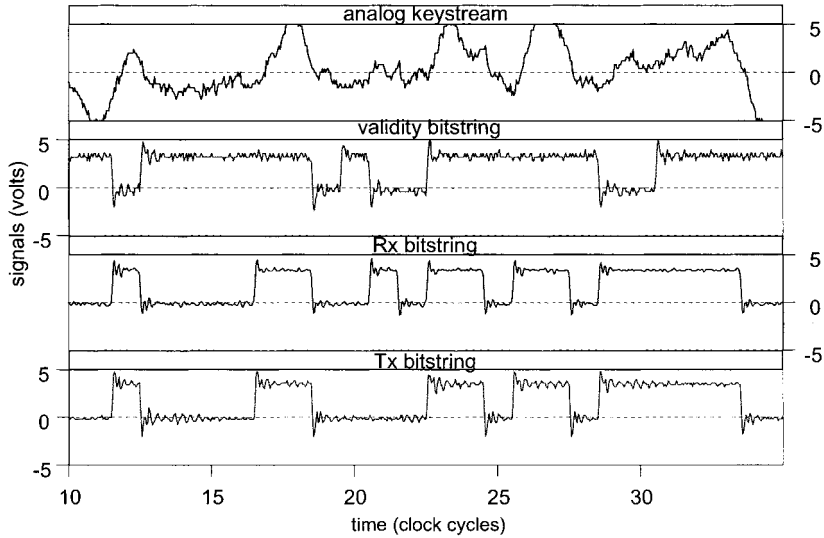

Fig. 5. Transmitter and receiver generated keystrings.

shows a sample of transmitter and receiver generated keystrings along with the analog keystream and the validity bitstring.

For this demonstration, the phase-noise lightwave was formed by filtering the optical noise generated by a free running fiber amplifier. The usual 50 nm wide amplified stimulated emission (ASE) was filtered to a bandwidth of about 1 nm, producing intensity modulations of ≈ 100 GHz. For our demonstration, the modulation bandwidth was filtered by the limited 100 MHz response of the photodetector and an electronic filter to about 10 MHz. One detected analog keystream is shown at the top of Fig. 5. The polarity of the noise is translated into the bit values of the keystrings. At the same time, a high validity bit assignment indicates that the magnitude of the noise is outside of a ~ 1 volt error prone zone near the discrimination threshold at 0 volts. It may be seen in this record that the Tx and Rx key bits disagree at the 21st clock cycle, probably due to noisy electronics. But, the validity bit is low in that slot, indicating that the key bit obtained at that time is to be discarded.

NETWORKS

QDRN is the only one of the three schemes that is compatible with networks. The others are sensitive to power level and cannot tolerate branching losses at the various junctions in the network.

A QDRN session works like this: Alice broadcasts the phase-noise lightwave to everybody, including unauthorized stations, if any. Then she chooses a key (interferometric settings) at random and conveys it to each authorized station one at a time using the scan technique described earlier. (Look out for ambiguous uses of the word "key". Some people use it for the whole 1TP, as in the name Quantum Key Distribution.) She conveys the key to each authorized station one at a time using the scan technique described earlier. These private sessions last only about one second each as discussed previously. As always, some sort of authentication is required to ensure that Eve is not among them. Each member of the session sends a list of invalid bits to everybody. By the time Bob and Alice have rejected the weakest ones, there are only a few left for Carl, Donna, and Elaine to reject, and so this should go quickly with the aid of data compression. At this point, all authorized members have the same 1TP and can proceed with their classified session.

QDRN AND LONG DISTANCE TRANSMISSION

An important issue is the ability to transmit the keystream over long distances. The concern is that the fiber dispersion, nonlinearity, and amplifier noise will alter the optical field enough to cause an excessive number of bit errors. We have not yet performed propagation experiments in re-entrant spools of fiber, but we did use a numerical model governed by the non-linear Schrödinger equation. The model includes fiber loss, dispersion, nonlinearity, amplifier gain, and spontaneous emission. To verify the model, we showed that it correctly propagates solitons, whose non-linear effects are far greater than those of interest here. The model also correctly reproduces 4-wave mixing and self-phase modulation as judged by comparing it with a wide variety of published experimental results. The amplifier spacing, noise figure, zero-dispersion wavelength and other parameters were also taken from published results. The computed SNR agrees with experiments within a couple of dB.

Figure 6 shows the points in the QDRN system where we computed two outputs to be compared, the analog keystreams as in Fig. 2. We put amplifiers at intervals of 60 km and assumed low-pass filtering to 2.5 Gbits/sec. At that time we were using 50 GHz instead of 100 as the bandwidth of the phase-noise lightwave. Figure 7 shows the result after propagating 660 km. The two waveforms remain substantially the same, and are clearly good enough to generate a 1TP using a modest threshold for validity.

A couple of other simple sanity checks are compatible with this conclusion. Malyon, Widdowson, and Lord[8] demonstrated digital pulse propagation over 20 megameters. Scaling this distance by the ratio of

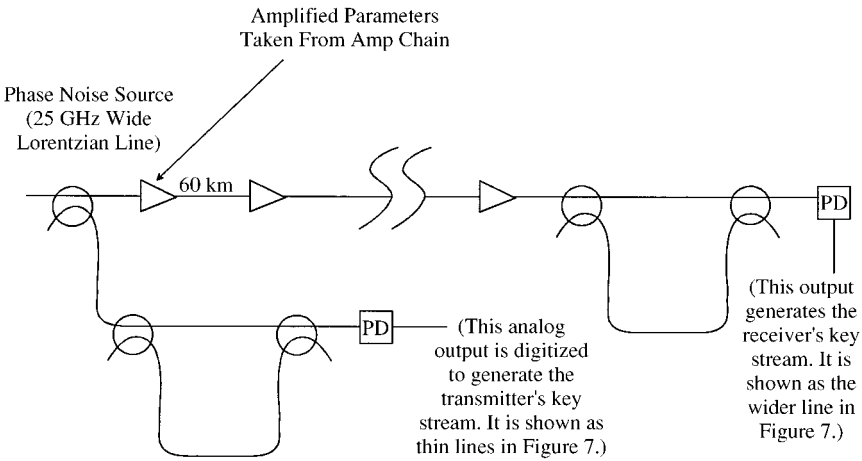

Fig. 6. Test points used in long distance numerical simulation.

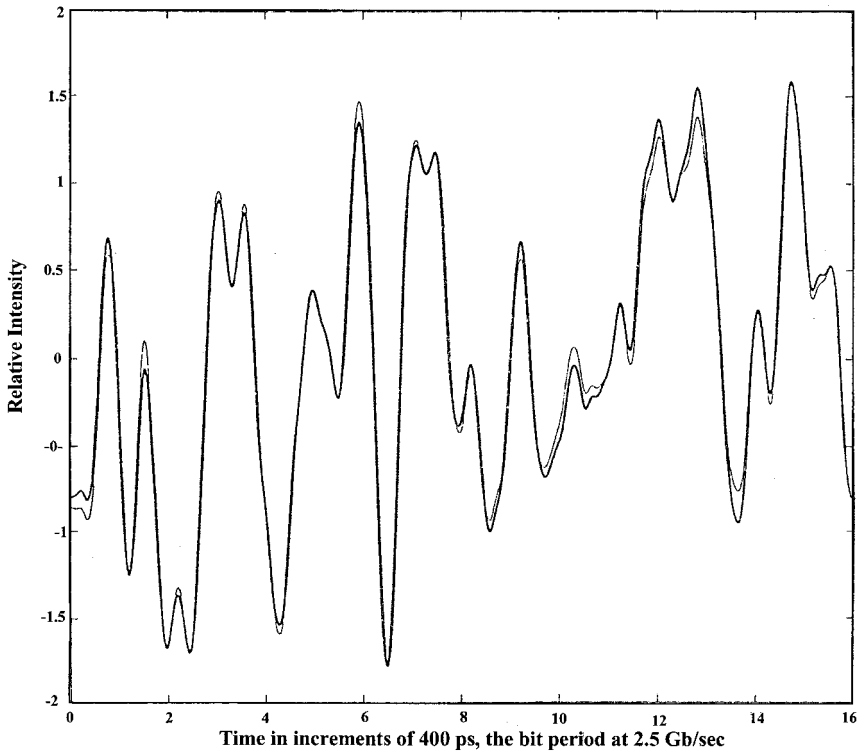

Fig. 7. Analog waveform at transmitter (thin line) and after 660 km (thick line).

bandwidths, 2.5 GHz/50 GHz gives us 1.0 Mm. For the greater bandwidth discussed in the main text, it would be 500 km.

Finally, let us make an estimate using dispersion only. Assume a typical dispersion slope of 0.06 ps/nm^2/km and say we are 2 nm off the zero-dispersion wavelength. Say the bandwidth is 50 GHz or 0.5 nm. The product of these numbers gives $\Delta t = 0.06$ ps/km. At 2.5 Gb/sec, a bit lasts 400 ps. Say we limit Δt to 60 ps, 1/7 of a bit. Then the transmission distance is 60 ps/ (06 ps / km) = 1000 km. Similarly a bandwidth of 100 GHz gives 500 km.

REMARKS ON QUANTUM CRYPTOLOGY (QC)

QC has severe drawbacks in regard to the generation, conservation, and detection of single photons per bit. This requires non-standard underdeveloped components and presents other formidable practical difficulties. This is offset to some degree by its absolute guarantee against passive eavesdropping. However, the absolute guarantee does not extend to the tamper-proof auxiliary link. Therefore, what QC really accomplishes is to ensure that Eve's attack, if any, will be against the auxiliary link, followed by the impersonation attack discussed earlier.

In comparing QC to classical schemes, it is useful to understand it in a simple semiclassical way rather than relying on the usual abstract descriptions such as in the one used by Bennett.[1]

Alice and Bob each have half of a Mach–Zehnder interferometer, Fig. 8, which they use as a phase-modulated communications link. The heuristic figure shows a dual transmission line, which in practice can be

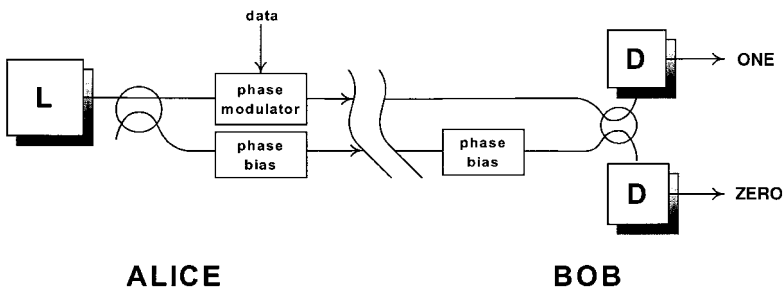

Fig. 8. PM Link.

replaced by other schemes, such as that of Bennett[1] or the Faraday mirrors of Zbinden *et al.*[2]

First we explain how the link works with classical power levels; then we reduce the power to show how it becomes secure at one photon per bit. Data pulses modulate the phase by 180°. Bob adjusts his phase biases so that ZERO bits come out his ZERO detector and ONEs exit from his ONE detector. Let us say that 0°-phase shift represents ZERO, and 180° represents ONE.

In an alternate mode of operation, Alice and Bob both shift their phase biases so that 90° represents a ZERO bit, and 270° a ONE. Next, they do something that at first seems very strange: they both independently switch modes at random. Their mode choices agree only half the time. For the other half, their phases are in quadrature and Bob gets half a pulse from each detector, no information. Bob makes a raw version of the pad with states ZERO, ONE, and INC (inconclusive). After the transmission Bob tells Alice which bits are INC. Finally they both discard these from their one-time pads, which they compress to fill the gaps.

Eve can defeat this scheme. She cuts the cable (or opens a connector somewhere) and installs her own repeater. It includes two receivers, one in each mode. She interprets both 0° and 90° as ZERO and 180° and 270° as ONE and thereby creates her copy of the one-time pad. Next she must deceive Alice and Bob. With quadrature phase measurements she has complete knowledge of the light's phase. She reconstructs the lightwave from Alice and sends it on to Bob with all the correct phase shifts. Finally she taps the public auxiliary link and learns which bits to discard from her replica of the one-time pad.

To claim victory, Alice sends only one photon per bit of information. When she and Bob are in opposite modes, 90° out of phase, Bob does not get half a photon at each detector. He gets the whole photon at one or the other, which looks like a valid bit. However, after the transmission he and Alice can still decide which bits are INC by exchanging lists of their modes by way of the auxiliary link.

Now Eve's second receiver is useless: she cannot receive half a photon in each one. Moreover, when she is in the wrong mode, 90° out of phase, she cannot know this by getting half a photon at each detector. Like Bob, she gets the single photon in one detector or the other and cannot decide whether her mode agrees with Alice's or not. Therefore, she sends bad data to Bob, for example 180° instead of 270°. Finally, Eve's deception is exposed when Alice and Bob compare notes on the tamper-proof auxiliary link. Knowing the one-time pad is compromised, they will never use it to encode secrets.

REMARKS ON THE YUEN–KIM PROTOCOL (YKP)

This is the easiest scheme to implement. However, people are a bit uncomfortable with its reliance on low power and noise statistics. Eve defeats it if she has a SNR greater than Bob's by at least 9 dB. Since Eve is free to move much closer to the transmitter than Bob, it is essential to keep strict control over its absolute power output. The length of a YKP transmission line is limited by the 9 dB. For optical fiber with attenuation 0.2 dB/km, this sets the maximum at 45 km.

We doubt whether YKP can benefit from an amplifier or analog repeater (definitely not a digital regenerator). Bob cannot distinguish between noise coming from the amplifier and noise from his own receiver. Therefore, Eve moves downstream from the amplifier where she gets partially the same noise that Bob gets. As a result the two of them select many of the same bits for their 1TPs, which compromises security.

Otherwise, Eve's best attack may be an opaque one in which she installs a repeater that takes all the light. After she selects bits for her 1TP, she must deceive Bob into selecting mostly the same ones. She relays her selected bits with extra signal strength and replaces the others with an average between ONE and ZERO. Bob can detect this deception only by statistical analysis that reveals a deviation from Gaussian noise.

Tomita and Hirota[4] discuss performance limited by both shot noise and thermal noise. However, they don't mention that the competition between Bob and Eve will drive both of them to use the most effective receiver, probably optical heterodyne with a laser local oscillator. The detector need not be cooled, because heterodyne gain overpowers thermal noise prior to detection. The effective noise at the input is well known:

$$N = h\nu[Bb]^{1/2}/\eta$$

where η is the detector's quantum efficiency, B is the optical bandwidth, and b the information bandwidth, If $B = b$ and $\eta = 1$, then this is essentially the quantum limit.

CONCLUSIONS

Three dissimilar schemes for secure optical communications exhibit the same curious attributes that one might think are unique to QC:

- All are invulnerable to passive eavesdropping.
- Users need no initial shared secret.
- Users do need an auxiliary tamper-proof link.
- The keystream is unusable until stored in a pad and processed.

QC is probably the least viable because one pays a high price for the care and nurturing of single photons. And for this price, one does not get an absolute guarantee of privacy except in an unusual case where something else provides an absolutely tamper-proof auxiliary link.

The advantage of YKP is simplicity. A drawback is strict control of the power level on the transmission line. This precludes network applications. The range of YKP is severely limited by the 9 dB requirement, about 45 km in optical fiber.

The main advantages of QDRN are compatibility with networks and the use of full power and typical high data rates. The distance falls in the range 500 to 1000 km. The price is the requirement for an uninterrupted coherent light path on a fiber with very limited dispersion and the need for advanced switching and stabilization of the interferometers.

REFERENCES

1. C. H. Bennett, *Phys. Rev. Lett.* **68**, 3121 (1992).
2. H. Zbinden *et al.*, *Elec. Lett.*, online #19970427 (1997).
3. H. P. Yuen and A. M. Kim, *Phys. Lett. A* **241**, 135–138 (1998). Errata: *Phys. Lett.* **A246**, 560 (1998). The subject of this reference is covered in Ref. 4 without errata.
4. A. Tomita and O. Hirota, *J. Opt B: Quantum and Semiclass* **Opt 2**, 705–710 (2000).
5. W. Wells, R. Stone, and E. Miles, *IEEE J. on Selected Areas in Communications*, **11**, 770–777 (June 93).
6. J. Menders, C. Diamond and E. Miles, *Algorithms and Systems for Optical Information Processing, V*, Proceedings of the SPIE, Vol. 4471 (2001).
7. J. Menders, Final Technical Report, CDRL ITEM A004, Secure Communication with QDRN, Feb. 2002.
8. Maylon, Widdowson and Lord, *IEEE Elec. Lett.*, **29**, 207 (1993).