JOURNAL OF MODERN OPTICS, 2001, VOL. 48, NO. 13, 2023–2038

Large pulse attack as a method of conventional optical eavesdropping in quantum cryptography

ARTEM VAKHITOV†, VADIM MAKAROV‡§ and DAG R. HJELME‡

†Department of Quantum Electronics, St Petersburg State Technical University (SPbSTU), Politechnicheskaya street 29, 195251 St. Petersburg, Russia

‡ Department of Physical Electronics, Norwegian University of Science and Technology (NTNU), N-7491 Trondheim, Norway

§http://www.vad1.com

(*Received 15 January 2001; revision received 12 June 2001*)

Abstract. In this paper so-called 'large pulse attack' is investigated. This attack is one of the possible methods of conventional optical eavesdropping, a new strategy of eavesdropping on quantum cryptosystems, which eliminates the need of immediate interaction with transmitted quantum states. It allows the eavesdropper to avoid inducing transmission errors that disclose her presence to the legal users. As an object of the eavesdropping, phase-state fibre optic schemes are considered. With large pulse attack, settings of transmitting and/or receiving apparatus are interrogated by external high-power light pulses. Applicability conditions of this method are given. Type and amount of information learned by the eavesdropper is estimated, depending on parameters of the interrogating pulse and apparatus. An experimental set-up for an eavesdropping experiment is proposed and results of successful preliminary measurements are presented. It is concluded that additional protection is necessary for currently implemented quantum key distribution systems. The paper suggests several security measures against this kind of attack.

1. Introduction

Many studies of eavesdropping in quantum cryptography have been made over the last few years [1–16]. In these papers, security of quantum cryptography against different kinds of quantum attacks was analysed—from simple beamsplitting and intercept/resend attacks to complex generalized joint attacks, which manipulate all transmitted quantum states as a whole. The eavesdropper's capabilities are typically assumed to be limited only by the laws of physics, not by the current level of technology, and in this paper we shall follow this tradition. Security of quantum cryptography was proven in general for all individual attacks [10, 11], where every single transmitted state is treated separately by Eve. It was also proven for all collective attacks [7, 13], where each transmitted state is attached to a separate probe, but after that, measurement is performed collectively on all probes. Finally, the proof was generalized for any eavesdropping attack [12, 15, 16], provided, however, an ideal single-photon source is used. Practical limits of security were established for the case of a noisy environment and imperfect

Journal of Modern Optics ISSN 0950–0340 print/ISSN 1362–3044 online © 2001 Taylor & Francis Ltd
http://www.tandf.co.uk/journals
DOI: 10.1080/09500340110074691

detection as well as non-ideal light sources [6, 8–11]. The common feature of all these attacks is the fact that Eve performs her measurements on the quantum states transmitted from Alice to Bob, therefore inevitably disturbing these states and inducing transmission errors. However, this is not the only possibility for eavesdropping on quantum key distribution (QKD) systems.

We will call *conventional optical eavesdropping* the strategy where Eve can get information by using loopholes in Alice's and Bob's optical set-up rather than by measuring the transmitted quantum states. Here are the possibilities we have found so far for this kind of eavesdropping.

(1) *Large pulse attack*. In a wide class of QKD schemes, the states forming the quantum alphabet are prepared by modulation of certain parameters of propagating light, such as polarization or phase. It can be done with phase modulators (e.g. Pockels cells) situated inside transmitter and receiver. With these kinds of QKD schemes, let us consider Eve launching a bright light pulse into the transmission line towards Alice's or Bob's set-up. Some part of this pulse will be reflected back from different optical components inside the set-up, because any real component has a non-zero reflection coefficient. On its way, the pulse can pass internal modulators and be modulated one or more times. Measuring characteristics of reflected pulses, Eve can make some conclusions on the modulator's settings and, as we will show later, if not learn the transmitted bits directly, then at least know transmission or detection bases, which will allow her to detect transmitted quantum states unambiguously. This attack was briefly mentioned in [17] and discussed a bit more in detail in a recent IBM paper [18], where it was called a 'large pulse attack'.

(2) *High-power destruction of optical components*. High-power external pulses can in principle make intentional changes in Alice's and Bob's optical components, which may facilitate further attacks. For example, damaging Alice's output attenuator in a way that will reduce its attenuation would make both beamsplitting (as well as other quantum attacks) and large pulse attack more efficient.

(3) *Light emission from avalanche photodiodes (APDs) during detection*. APDs are currently used as single-photon detectors in QKD schemes. An APD junction emits light over a broad spectrum during avalanche [19]. Part of this light leaks back into the communication fibre, where it can be detected by Eve. A recent study hints that the amount of light leaking back into the APD fibre pigtail is a few orders of magnitude less than one photon per avalanche [20]. However, more studies are necessary, notably for InGaAs detectors over a wide emission spectral range including wavelengths longer than 1.6 μm, which currently presents some experimental difficulty.

In this paper, we will consider in detail the first of these possibilities—large pulse attack, including several important features that have been missed in the two papers [17, 18] mentioned above. We will restrict our study to fibre-optic phase state QKD systems using protocols BB84 [21] and B92 [22]. As an example, Townsend's scheme [23] will be considered, but most results are also applicable to other existing fibre-optic and free-space QKD schemes. A special discussion will be devoted to 'plug & play' schemes [17, 18].

2. Eavesdropping set-up

The general structure of the eavesdropping set-up for performing large pulse attack is shown on figure 1. Light pulses emitted by the laser are divided into scanning and reference pulses on the coupler. Scanning pulses propagate towards Alice's or Bob's set-up through the optical multiplexer, then, after reflecting back, through the same multiplexer and coupler, enter the detection scheme. We assume that Eve will use the most sensitive detection method, i.e. homodyne detection, and hence will need reference pulses. They are delayed in the reference arm to arrive at the detection scheme simultaneously with the chosen reflected pulses. The particular content of the detection scheme depends on what parameter of the signal Eve measures. The optical multiplexer is necessary for the photons sent by Alice to pass undisturbed to Bob.

If only time domain multiplexing is used, it may cause problems due to Rayleigh backscattering: if Alice's photon and Eve's scanning pulse meet somewhere, then some amount of backscattered light from the scanning pulse can reach Bob's detector, which is undesirable to Eve, because it can cause additional detection errors at Bob. Eavesdropping on a wavelength different from that used for transmission and, correspondingly, wavelength domain multiplexing can eliminate this effect.

Before starting to consider how Eve can extract information in phase state QKD systems, we should explain the necessary details of phase modulator operation and also make some assumptions.

Standard telecommunication voltage-controlled phase modulators would normally be used in Alice's and Bob's set-ups. With the BB84 protocol, there are four voltage levels corresponding to the four possible values of phase shift used at Alice's modulator, and two levels used at Bob's modulator corresponding to the two possible detection bases. With B92, two voltage levels on either side are used. All these voltage levels change in a random order from one bit to another, according to the protocol. Let us call *transmission cycle* the full time interval needed for transmission of a single bit. In figure 2, two sequential transmission cycles are presented. Each transmission cycle consists of three parts.

(1) Rise time or fall time, depending on whether the phase shift value in the previous cycle corresponds to a lower or a higher voltage level. The parameter τ_{rf} will denote here the longest possible rise/fall time.
(2) Settling time. For correct detection, phase shift at the modulator must be set with certain precision (estimates made for our QKD set-up [24] require

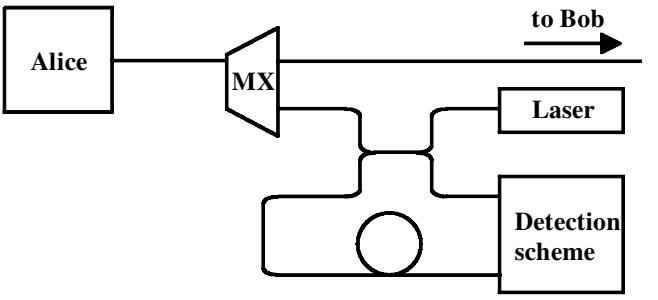

Figure 1. General structure of eavesdropping set-up.

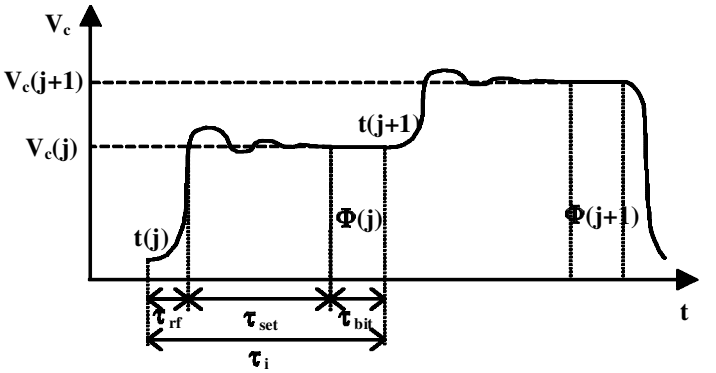

Figure 2. Transmission cycle and time parameters.

precision of about $\pm(5-10)^\circ$). The control voltage cannot settle immediately to the required accuracy, and during a certain period of time denoted τ_{set} some ringing will always occur.

(3) Bit slot, during which a photon passes the modulator and acquires phase shift. This time is denoted as τ_{bit}.

Besides this, $t(j)$ and $t(j+1)$ denote the beginning of the jth and the $(j+1)$th transmission cycles, correspondingly, $\Phi(j)$ and $\Phi(j+1)$ are phase shifts coding the information bits transmitted in these cycles, and $V_{\text{c}}(j)$ and $V_{\text{c}}(j+1)$ are the corresponding phase modulator voltages.

Assumptions and constraints to Eve's interrogation pulses.

(a) First, it is clear that Eve's pulses should not pass modulators during the rise/fall time of the control voltage, otherwise her measurement will be greatly complicated.

(b) The situation when the phase modulation efficiency for Eve's pulses and for transmission pulses is the same results in some special cases that we consider below. We will assume this by default. Modulation efficiency will be the same if Eve's interrogation wavelength is close to Alice's transmission wavelength.

(c) If Eve chooses not to employ wavelength domain demultiplexing, her pulses must not coincide in time with photons transmitted as they exit Alice's set-up, otherwise she will not be able to separate them. That is to say, Eve's pulses being *on the way out* must not pass the modulator during the bit slot. Thus, the only time interval allowed here is τ_{set}. With wavelength domain multiplexing, this constraint is not necessary.

(d) Since positions of reflecting elements inside Alice's and Bob's set-ups are not in Eve's control, she will not always be able to arrange her measurements in such a way that her pulses will pass the modulator during the bit slot or very close to it. In many cases this will occur in the middle or even at the beginning of the settling time. Oscillations of control voltage during this interval can result in phase errors of 10°–20° (according to the measurements made on our own set-up), but this is acceptable for Eve since she does not need high accuracy to learn most of the bits, and it also helps that she uses multiphoton pulses.

(e) Eve may be practically tempted to use as wide interrogation pulses as possible to increase their energy and level of the signal she has to detect. We will neglect the facts that Eve's interrogating pulses have a non-zero width and the control voltage varies during τ_{set}.

Each of the interrogation pulses sent by Eve will produce a number of reflected pulses. The most important characteristics of these reflected pulses are (a) resulting phase shift acquired by them due to the modulation(s) in Alice's or Bob's set-up, and (b) delay between two successive modulation events in the case of multiple modulation. These characteristics, which Eve must consider given, determine what information Eve can learn by detecting a specific reflected pulse. Here we restrict ourselves to the cases of single and double modulation. Three scenarios are then possible for Eve: (a) learning transmission/detection bases; (b) guessing the raw key from a few possible variants; and (c) learning the raw key immediately.

3. Direct and indirect detection of information bits

To get the raw key directly, Eve can detect the pulses reflected from Alice's set-up and modulated only once during their travel inside it (if such pulses exist). It is clear that the modulation in this case must occur *either* on the way in, before the reflection, *or* on the way out, after the reflection. The possible values of the phase shift can be determined unambiguously, assuming that the bright interrogation pulses sent by Eve return her multiphoton reflections.

Consider now an interrogation pulse launched by Eve into Alice's set-up and modulated there twice during two adjacent transmission cycles: first time on the way in, during τ_{set} or the τ_{bit} time slots of the first transmission cycle, and second time on the way out, during τ_{set} or the τ_{bit} time slots of the second transmission cycle (see figure 3). Note that if only time-domain multiplexing is used, the second τ_{bit} interval must be excluded because the reflected pulse must not coincide in time with Alice's transmitted photon, as mentioned above. The delay between the two modulation events will be further referred to as $2\tau_R$. Neither of these events must occur during the τ_{rf} slot, so the general constraint for the delay in this case is

$$\tau_{rf} < 2\tau_R.$$

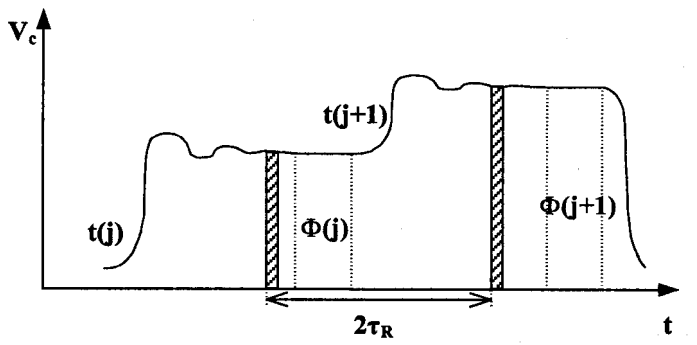

Figure 3. Eve's pulse passing the phase modulator for indirect detection of information bits.

Table 1. Illustration of indirect detection of information bits (BB84).

Alice's bits	1	0*	0	1	1*
Alice's phase shifts	π	$\pi/2$	**0**	π	$3\pi/2$
Phase shifts detected by Eve	—	$3\pi/2$	$\pi/2$	π	$\pi/2$
Possibilties for phase shifts	0?	$3\pi/2$	π	0	$\pi/2$
in key sequence	$\pi/2$?	π	$3\pi/2$	$3\pi/2$	π
	$3\pi/2$?	0	π	0	$\pi/2$
	π?	$\pi/2$	**0**	π	$3\pi/2$

The phase shift acquired by Eve's pulse will be equal to the sum of phase shifts in both transmission cycles:

$$\Phi_{\mathrm{E}} = (\Phi(j) + \Phi(j+1)) \bmod 2\pi.$$

Note that the value of Φ_{E} itself will be equal to one of the possible phase shift values used in the protocol. Detection of this phase shift will give Eve an ambiguous result, because she does not know the phase shift acquired in the first transmission cycle. However, there are only a few possible values for this phase shift, i.e. four in BB84 and two in B92. It means that Eve will have to guess the right key sequence from only four or even two variants. In practical cryptography, this is equivalent to the knowledge of the key. Table 1 illustrates this guessing procedure.

The above discussion is also applicable to interrogating Bob's modulator, but only with the B92 protocol, since in BB84 Bob's phase shifts determine only detection bases, not bit values.

What if $2\tau_{\mathrm{R}}$ is so long that the two modulation acts are not in adjacent transmission cycles? In general, if the first modulation act happens in the jth transmission cycle and the second in the $(j+n)$th transmission cycle, then the number of possible key sequences is 4^n for BB84 and 2^n for B92.

If, however, Eve is using a substantially different wavelength, then it might happen, due to different phase modulation efficiency for her pulse, that even with double modulation she can learn information bits, not only bases.

4. Detection of transmission bases

Security of the BB84 protocol, at least in the QKD schemes considered now, is based on the fact that during the transmission Eve knows neither bases in which Alice encodes key bits nor bases in which Bob attempts to detect them. If Eve somehow manages to get the value of either Alice's or Bob's basis *before* Alice's photon reaches Bob's location, then the whole scheme is no longer secure, and Eve can implement an ideal 'intercept/resend' attack without being caught. Now we will show that determining transmission and/or detection bases is possible by means of large pulse attack.

(1) The first and also obvious case is when Eve's pulse is modulated once during its travel inside *Bob's* set-up, and two possible values of acquired phase shift correspond to Bob's two possible detection bases. Similarly to the case of direct detection of information bits, Eve's pulse passes Bob's modulator *either* on the way in *or* on the way out, but not on both. If τ_{PM} is

the time required for an optical pulse to propagate from Eve to Bob's phase modulator, and τ_{back} is the time required for the pulse to propagate back to Eve after the reflection, then the condition for a successful attack is

$$\tau_{\text{R}} + \tau_{\text{back}} + \tau_{\text{PM}} < \tau_{\text{set}}.$$

One can easily check that if this condition is satisfied, Eve will have enough time to receive the reflected pulse modulated in Bob's modulator during τ_{set}, determine Bob's detection basis that he is preparing to use, then 'catch' Alice's photon before it enters Bob's site, detect it in this basis, and re-send it further to Bob in this basis. This way, Eve ideally never causes additional errors that would reveal her presence.

(2) If Eve's pulse is modulated twice inside Bob's set-up, once before and once after being reflected, so that both modulation events occur during the τ_{set} time interval for a the same transmission cycle, then the condition of successful attack will be

$$2(\tau_{\text{R}} + \tau_{\text{PM}}) < \tau_{\text{set}}.$$

(3) Yet another case is when the interrogation pulse is modulated twice inside *Alice's* set-up, once before and once after being reflected, so that the modulation events occur during the τ_{set} time interval of the same transmission cycle (see figure 4). Parameter τ_{R} of the chosen reflected pulse must satisfy the condition

$$2\tau_{\text{R}} < \tau_{\text{set}}.$$

In cases 2 and 3, the value of the phase shift acquired by the pulse will double:

$$\Phi_{\text{E}} = 2\Phi(j) \bmod 2\pi.$$

It is easy to see that the resulting phase value will be determined by the transmission or detection basis: $\Phi_{\text{E}} = 0$ if $\Phi(j) = 0$ or π, and $\Phi_{\text{E}} = \pi$ if $\Phi(j) = \pi/2$ or $3\pi/2$.

Let us also note that Eve's intercept/resend equipment in practice would introduce additional delay to the transmitted photons. If we assume that propagation delay for all communication between Alice and Bob is not authenticated, then Eve can introduce a constant delay into all communication between them to compensate for her processing delay. Alternatively, Eve can exploit the fact that the signal propagation speed in a free-space radio link is faster than that in optical

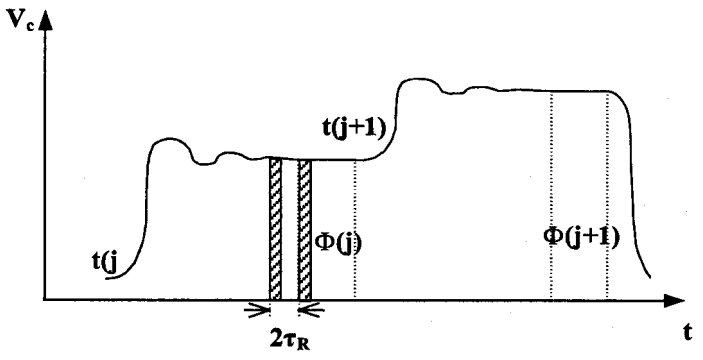

Figure 4. Eve's pulse passing the phase modulator for bases detection.

fibre, and employ such radio links in her set-up to cancel her processing delay [25]. An appropriately constructed electrical cable connection could also be used.

5. Notes on bases detection at Bob's site

It should be pointed out that even if Eve gets information about detection basis only after the photon enters Bob's site, she can still learn some additional information about the key. Let us consider Eve performing, in addition to detection of transmission bases at Bob's site, the well-known beamsplitting attack. The following is typically assumed [18].

(1) If f is the fraction Eve is splitting off from each transmitted pulse and μ is the average photon number per pulse, then she will get a fraction $[1 - \exp(-f\mu)]$ of all transmitted pulses, or $\sim f\mu$ for small $f\mu$. This gives Eve a fraction $f\mu/2$ of the error-corrected key, where the factor of $\frac{1}{2}$ is due to the necessity of applying random detection bases to split pulses.
(2) If Eve tries to store photons until the public discussion, when the bases are announced, Alice and Bob can always delay this discussion by arbitrary time sufficient for most stored photons to decay.

However, if τ_{PM}, τ_{back} and τ_R delays in Bob's set-up are such that Eve gets basis information in a short time after the transmitted pulse has left her location, then Eve can simply delay the split pulse for this short time and after that detect it in the correct basis. Thus, with bases detection the estimate of $f\mu/2$ is wrong, and it should be assumed that Eve can obtain the whole $f\mu$ fraction of the transmitted key through a beamsplitting attack, which is the same as if she were granted the ability to store photons for unlimited time.

6. Security measures

The greater part of this section will assume the BB84 protocol, and only the last paragraphs will be devoted to B92.

As a security measure against large pulse attack, it was proposed in [17, 18] for 'plug & play' systems to monitor intensity of incoming light in Alice's set-up, presumably over a wide range of wavelengths. In these systems, which are essentially asynchronous, *Bob* first sends to Alice relatively intense light pulses, which serve *inter alia* to provide synchronization signals upon registering by a special timing detector in Alice's set-up (figure 5). Thus, one can make this detector alarm honest participants when average power and/or peak intensity of an incoming pulse rises above a specified level. However, attention was not paid to the fact that the system remained insecure against detection of transmission bases at Bob's site.

We will now offer simple passive security measures against large pulse attack. These measures are different for Alice and Bob.

For practical security of Bob's site against detection of *transmission bases*, it would be sufficient that, for any possible potentially 'harmful' reflection, one of the following conditions is satisfied:

$$\tau_R + \tau_{back} + \tau_{PM} > \tau_{set}$$

or

$$2(\tau_R + \tau_{PM}) > \tau_{set},$$

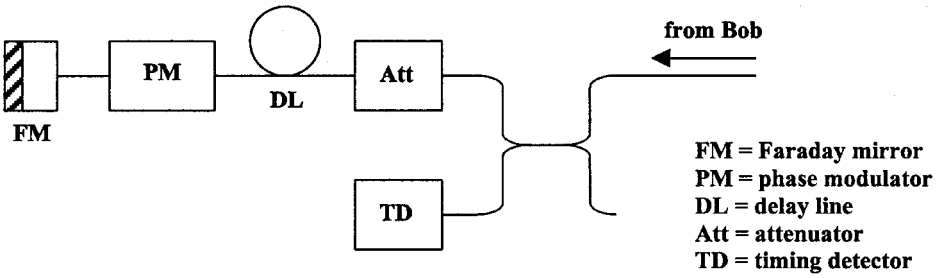

Figure 5. Alice's set-up in the 'plug & play' scheme.

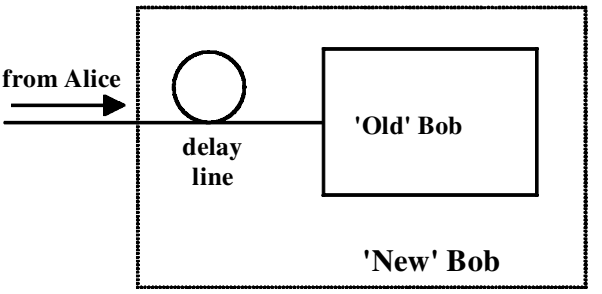

Figure 6. Passive security measures for Bob's set-up.

depending on the type of large pulse attack (single or double modulation, respectively). Normally, Bob will not know Eve's position, but it is enough to satisfy the inequalities assuming that she is sitting right at the input of Bob's set-up. If they are not satisfied, the solution is to put a delay line of appropriate length at the input of Bob's set-up (inside the secure site), thereby increasing τ_{back} and τ_{PM} delays, as shown on figure 6. Really, if one makes this delay line long enough to provide one-directional propagation delay of $\tau_{\text{set}}/2$, security conditions will be automatically satisfied. In fact, in many high-speed QKD systems this condition will be satisfied without any additional delay line, but one should be aware of the problem. This solution can be applied to any QKD scheme, including 'plug & play'.

The problem of security of Bob's site against direct and indirect detection of *information bits* appears only with the B92 protocol and will be discussed later.

The passive measures for Alice's site described below are not suitable for 'plug & play' systems, so the proposals made in [17, 18] are still valid. Now our description will concern Townsend's scheme.

First, the existing set-up must be slightly revised. In practice, instead of true single-photon states, Alice uses weak coherent pulses prepared by attenuating light from a laser to average intensity of about 0.1 photon per pulse. The attenuator can be situated immediately at the laser output (upper half of figure 7) or at the very output of Alice's set-up (lower half of figure 7), and there is no obvious reason not to do it the latter way. Indeed, for Eve this will mean a significant increase of power required of her laser: namely, if the attenuator at the output of Alice's set-up is set to A dB, then Eve's required laser power increases by $2A$ dB at once. In our QKD set-up [24], a standard telecommunication laser diode is used as the light

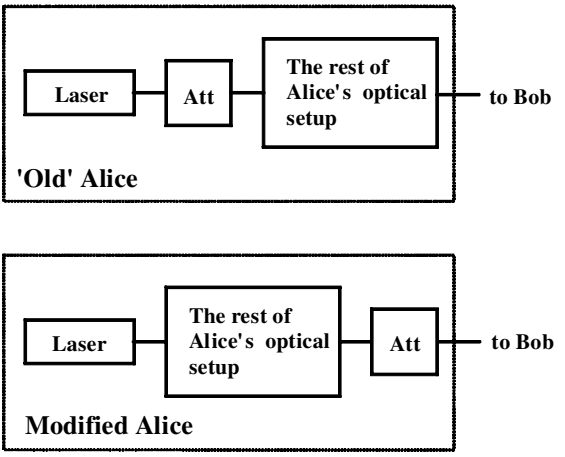

Figure 7. Modification of Alice's set-up.

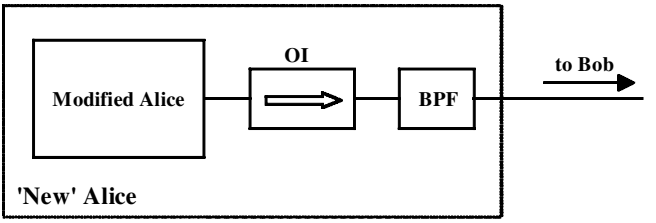

Figure 8. Passive security measures for Alice's set-up.

source (1310 nm, 100 ps wide pulses of about 1 mW peak power), and the output attenuator is set to about 60 dB, which introduces 120 dB of attenuation for Eve's pulse. We will refer to this set-up as the 'modified Alice's set-up'.

Then, we must add a couple of optical components. In figure 8, Alice's set-up modified as described above is connected with the communication channel through an optical isolator (OI) and band-pass filter (BPF). The optical isolator does not affect much the signal propagating from Alice, but strongly reduces the signal propagating in the opposite direction (for existing isolators, attenuation is about 50 dB). Efficiency of this device is wavelength dependent (its characteristics are typically stable in a range of several tens of nanometres), but the band-pass filter helps to cope with this problem. Thus, this construction introduces an overall attenuation $A_{\text{sum}} \approx 120 + 50 = 170$ dB for the pulse interrogating Alice's set-up. Now we can make an estimate of the minimum required laser power for Eve.

The following equation holds:

$$\mu h\nu = 10^{(-A_{\text{sum}}/10)} RP\tau,$$

where μ is the minimum average photon number per pulse that Eve requires for successful detection, h is Planck's constant, ν is the optical frequency, R is the coefficient of reflection from the rest of Alice's set-up, P is the peak power of Eve's interrogation pulse and τ is the width of Eve's interrogation pulse. Then the minimum peak power of Alice's interrogation pulse will be

$$P = \mu h\nu (10^{(-A_{\text{sum}}/10)} R\tau)^{-1}.$$

Let us assume $A_{\text{sum}} = 170\,\text{dB}$, $R = 1$ (really it is less than 0.1), $\nu = 10^{14}\,\text{Hz}$ (near infrared radiation), $\mu = 1$, and calculate P for two values of τ: $\tau_1 = 10^{-10}\,\text{s}$ (this is a typical width of pulses used by Alice and Bob) and $\tau_2 = 10^{-8}\,\text{s}$ (because Eve may want to use a broader pulse to increase its energy). By an order of magnitude, $P(\tau_1) \sim 10^8\,\text{W}$ and $P(\tau_2) \sim 10^6\,\text{W}$.

As you may see, even with our somewhat conservative assumptions, such a high-power fibre-optic laser, which Eve needs, is something close to science fiction (the most powerful commercially available fibre-optic pulsed lasers have peak power of about 1–10 kW [26]). Nevertheless, to make things more demonstrative, let us now calculate the power density S it would induce in the fibre, assuming a typical core area of $\sigma^2 = 100\,\mu\text{m}^2 = 10^{-6}\,\text{cm}^2$:

$$S(\tau_1) = P(\tau_1)/\sigma = 10^8\,\text{W}/10^{-6}\,\text{cm}^2 = 10^{14}\,\text{W cm}^{-2}$$

and

$$S(\tau_2) = P(\tau_2)/\sigma = 10^6\,\text{W}/10^{-6}\,\text{cm}^2 = 10^{12}\,\text{W cm}^{-2}.$$

Thus, even for long pulses, the required power density will significantly exceed the damage threshold of the fibre, which we assume is about $10^9\,\text{W cm}^{-2}$.

Let us remind the reader that these estimates are valid for Townsend's scheme with an attenuated light source. If, however, one uses a *true* single-photon source instead of an attenuated light source, then it makes no sense to put an attenuator at Alice's output, and the proposed protection is not applicable. Also, round-trip systems like 'plug & play' do not allow the use of non-reciprocal devices such as optical isolators, and this is why our solution for Alice is not suitable for 'plug & play' systems.

If the B92 protocol is used instead of BB84, it makes it more difficult to defend Bob's site against large pulse attack. Eve can now learn information bits by interrogating Bob, not only detection bases. Passive security measures against it are impractical, because any additional component will introduce loss and thus impair the maximum transmission distance and key generation speed. We cannot put an attenuator at the input of Bob's set-up, like we did with Alice, and an optical isolator itself does not have enough attenuation to provide security. Thus, one has to monitor the intensity of the incoming light. Bob will have to split off some part of the incoming light (figure 9) to a special sensitive alarm detector (AD) and probably install additional components into the optical path. Note that Eve can interrogate Bob's site with signals of very low intensity.

Unlike 'plug & play' systems, Townsend's scheme allows here the variation shown on figure 10, which reduces requirements to sensitivity of Bob's alarm detector. The incoming light propagates freely in an optical circulator (OC) from port 1 to port 2 and then to Bob's 'old' set-up, and most of the reflected light propagates from port 2 to port 3 to the alarm detector (Det). The optical band-pass filter (BPF) serves to compensate somewhat for changes in the characteristics of the optical circulator at different wavelengths.

To conclude, using the B92 protocol does not seem very practical. Luckily, it is also considered less secure for other reasons and is rarely used now.

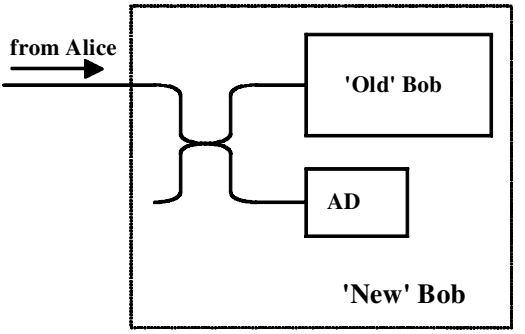

Figure 9. Active security measures for Bob's set-up with the B92 protocol.

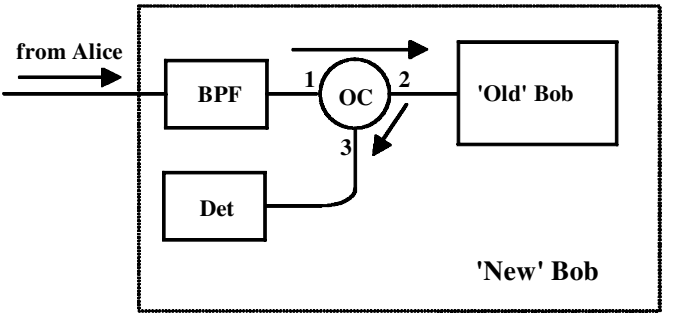

Figure 10. Active/passive security measures for Bob's set-up with the B92 protocol, with low additional losses and weaker requirements to the sensitivity of the alarm detector.

7. Simple experiment

Reflection coefficients of modern optical components are indeed made very low thanks to good anti-reflection coatings, but they are non-zero anyway. It is also good to remember that an anti-reflection coating is made for specific wavelengths, so if Eve chooses for interrogation a wavelength different from that specified for the coating, then she can get much larger reflection. Figure 11 shows typical values of return loss for different optical components. As one can see from the chart, the most suitable reflecting components for large pulse attack are free fibre ends, non-angled polished optical connectors, lasers and detectors. All in all, large pulse attack seems to be extremely feasible.

We arranged a simple experiment using the optical part of our QKD scheme [24], which has a structure similar to Townsend's system. The experimental set-up is shown on figure 12. Eve's equipment is built around a standard optical time domain reflectometer (OTDR)—millimetre resolution OTDR system produced by Opto-Electronics, Inc., which in this configuration provides us with a medium-power 1300 nm pulsed laser, sensitive time-selective detector and 50/50 coupler. Eve's laser pulses are divided on the coupler into a scanning and a reference pulse. After entering Alice's half of the interferometer, the scanning pulse propagates through its long arm which contains the phase modulator, and after being reflected from the free fibre end it propagates back through the same arm. We should note that reflection from the free fibre end in our QKD scheme existed well before we

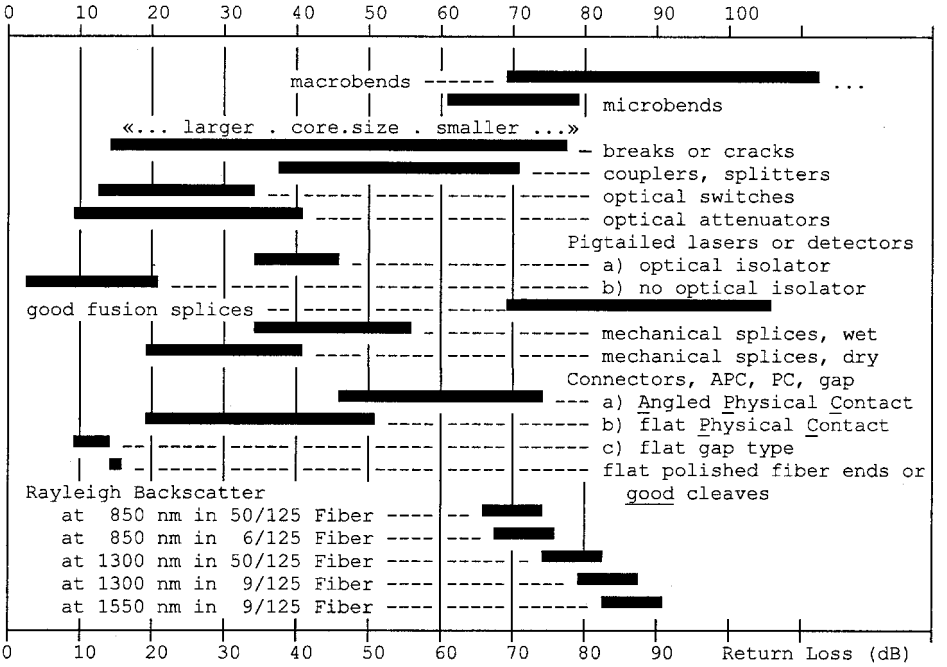

Figure 11. Typical values of reflection coefficients for different fibre-optic components. Courtesy of Opto-Electronics, Inc. (http://www.opto-electronics.com/).

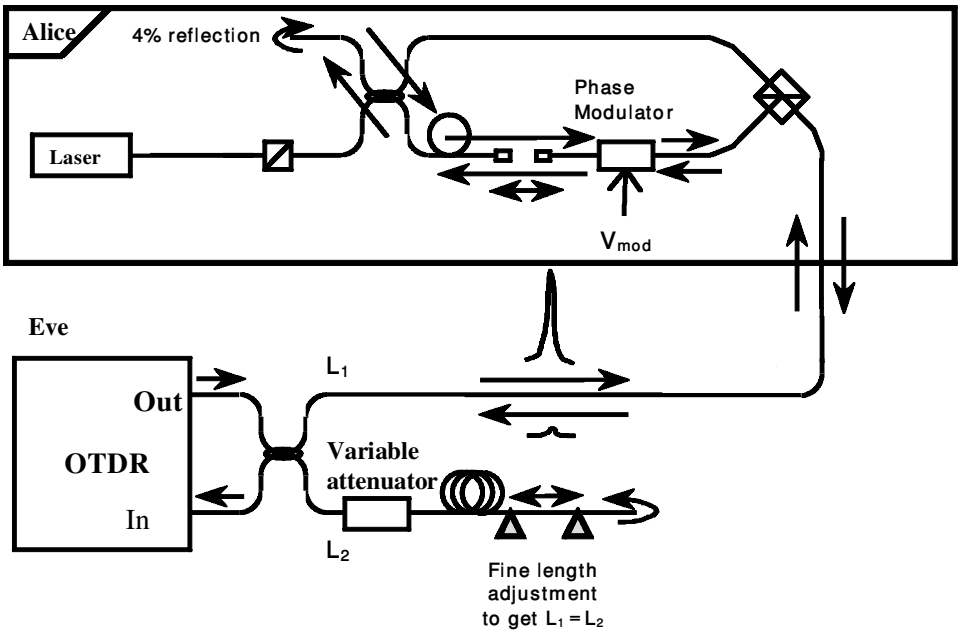

Figure 12. Schematic of our eavesdropping experiment. Interrogating Alice's phase modulator.

realized it could be used by Eve, as were several other reflections. The returned scanning pulse at the input of the OTDR detector was delayed by 88.85 ns and its level relative to the outgoing scanning pulse was −58 dB. The reference pulse was attenuated to the same level and delayed for the same time, to obtain interference with high fringe visibility on Eve's coupler. Polarization controllers not shown on the figure were used to steer the scanning pulse into Alice's proper arm and to match the polarization of the reflected and the reference pulses. The result of interference between reflected and reference pulses was registered by an APD-based detector. Since the laser that we used did not have enough power and the OTDR system was indeed not optimized for eavesdropping tasks, we removed the optical attenuator from Alice's set-up; no other changes to it were made.

Assuming the BB84 protocol, four static voltage levels were used to control the phase shift on Alice's modulator: 0, 2, 4 and −2 V, which corresponded to phase shift values for a scanning pulse of 0, $\pi/2$, π and $3\pi/2$. A static modulator voltage is equivalent to one infinite transmission cycle, so the experiment reproduces the situation with bases detection. Applying these static voltages, we observed constructive interference when the phase shift on the modulator was 0 or π, and destructive interference when the phase shift was $\pi/2$ or $3\pi/2$. Fringe visibility was about 0.9, and the phase drift constant was around $2\,\mathrm{min}/2\pi$ by its order of magnitude (some thermo-isolation was used for Eve's reference arm to slow the phase drift down). Thus, the experiment confirmed that remote reading of internal modulator settings by an external optical pulse is possible.

8. Conclusions

The following important conclusions can be made on large pulse attack and conventional optical eavesdropping (statements regarding Townsend's scheme may be applicable to other fibre-optic [27–29] and free-space [30] schemes, and of course to the original ones [21, 22]):

(1) QKD systems without internal optical modulators such as the Koashi–Imoto set-up [31] or EPR-based systems [32] are intrinsically immune to large pulse attack, because signals reflected from these systems cannot carry any information on quantum states transmitted. However, only one such system has been recently implemented [33].
(2) The BB84 protocol is generally preferable over B92. With Townsend's scheme, B92 does not allow passive security measures for Bob's set-up. With 'plug & play' schemes, B92 places strong requirements on the sensitivity of Bob's alarm detector.
(3) Large pulse attack with bases detection can double the amount of information that Eve obtains through a conventional beamsplitting attack. Note that granting Eve the ability to store photons for unlimited time leads to the same result.
(4) Security measures against large pulse attack include the following.
    (a) For Townsend's scheme with the BB84 protocol—passive measures both for Alice (figure 8) and Bob (figure 6). *It seems to be the easiest scheme to protect.*
    (b) For Townsend's scheme with the B92 protocol—passive measures for Alice (figure 8) and active/passive for Bob (figure 10).

(c) For 'plug & play' schemes with the BB84 protocol—active measures for Alice (figure 5) and passive for Bob (figure 6).
(d) For 'plug & play' schemes with the B92 protocol—active measures both for Alice (figure 5) and Bob (figure 9).

(5) Using a true single photon source (except in EPR-based schemes) will make passive defense of Alice's site against large pulse attack impossible.
(6) Feasibility of large pulse attack is experimentally confirmed.
(7) Further studies are required on the methods of conventional optical eavesdropping other than large pulse attack, such as light emission from an APD and high-power destruction of optical components.

To answer skeptics, we do believe that quantum cryptography is secure, but there are more issues to be carefully considered.

Acknowledgments

The study was supported by the Norwegian Research Council (NFR), project no. 119376/431; visit our project Web site at http://www.fysel.ntnu.no/Optics/qcr/ We also thank Andre Mlonyeni, Telenor R&D and Professor S. Cova, Politecnico di Milano for helpful discussions.

References

[1] Huttner, B., and Ekert, A. K., 1994, *J. mod. Optics*, **41,** 2455.
[2] Bennett, C. H., Brassard, G., Crepeau, C., and Maurer, U. M., 1995, *IEEE Trans. Inf. Theory*, **41,** 1915.
[3] Fuchs, C. C., and Peres, A., 1996, *Phys. Rev.* A, **53,** 2038.
[4] Hwang, W. Y., and Koh, I. G., 1997, quant-ph/9702037 v2.
[5] Lütkenhaus, N., 1996, *Phys. Rev.* A, **54,** 97.
[6] Mayers, D., and Yao, A., 1998, quant-ph/9809039.
[7] Biham, E., and Mor, T., 1997, *Phys. Rev. Lett.*, **78,** 2256.
[8] Brassard, G., Lütkenhaus, N., Mor, T., and Sanders, B. C., 1999, quant-ph/9911054.
[9] Dusek, M., Jahma, M., and Lutkenhaus, N., 1999, quant-ph/9910106.
[10] Lütkenhaus, N., 1999, quant-ph/9806008 v2.
[11] Lütkenhaus, N., 2000, quant-ph/9910093 v2.
[12] Mayers, D., 1998, quant-ph/9802025 v4.
[13] Biham, E., Boyer, M., Brassard, G., van de Graaf, J., and Mor, T., 1998, quant-ph/9801022.
[14] Yuen, H. P., 1996, *Quantum semiclass. Optics*, **8,** 939.
[15] Biham, E., Boyer, M., Oscar Boykin, P., Mor, T., and Roychowdhury, V., 2000, *Proceedings of the Thirty-Second Annual ACM Symposium on Theory of Computing*, Portland, Oregon, USA, 21–23 May, New York: Association for Computing Machinery, pp. 715–724.
[16] Shor, P., and Preskill, J., 2000, *Phys. Rev. Lett.*, **85,** 441.
[17] Ribordy, G., Gautier, J.-D., Gisin, N., Guinnard, O., and Zbinden, H., 2000, *J. mod. Optics*, **47,** 517.
[18] Bethune, D. S., and Risk, W. P., 2000, *IEEE J. quantum Electron.*, **36,** 340.
[19] Lacaita, A. L., Zappa, F., Bigliardi, S., and Manfredi, M., 1993, *IEEE electron. Devices*, **40,** 577.
[20] Kurtsiefer, C., Zarda, P., Mayer, S., and Weinfurter, H., 2001, *J. mod. Optics* '*Technologies for Quantum Communications*', to appear.
[21] Bennett, C. H., and Brassard, G., 1984, *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, pp. 175–179.

[22] Bennett, C. H., 1992, *Phys. Rev. Lett.*, **68,** 3121.
[23] Marand, C., and Townsend, P. D., 1995, *Optics Lett.*, **20,** 1695.
[24] Results of our work are not published yet, but some information is available at http://www.fysel.ntnu.no/Optics/qcr/
[25] Vakhitov, A., 2000, MSc thesis, Department of Quantum Electronics, St. Petersburg State Technical University: available at http://www.fysel.ntnu.no/Optics/qcr/ artem/
[26] See, for example, pulsed erbium fibre laser ELPD-1K, http://www.ire-polusgroup.com/erbLas/EFLGuide.htm
[27] Zbinden, H., BehcmannPasquinucci, H., Gisin, N., and Ribordy, G., 1998, *Appl. Phys.* B, **67,** 743.
[28] Sun, P. Ch., Fineman, E., and Mazurenko, Yu., 1995, *Optics Spectrosc.*, **78,** 887.
[29] Mérolla, J.-M., Mazurenko, Yu., Goedgebuer, J.-P., and Rhodes, W. T., 1999, *Phys. Rev. Lett.*, **82,** ??.
[30] Jacobs, B. C., and Franson, J. D., 1996, *Optics Lett.*, **21,** 1854.
[31] Koashi, M., and Imoto, N., 1997, *Phys. Rev. Lett.*, **79,** 2383.
[32] Ekert, A., 1991, *Phys. Rev. Lett.*, **67,** 661.
[33] Ribordy, G., Brendel, J., Gautier, J.-D., Gisin, N., and Zbinden, H., 2001, *Phys. Rev.* A, **63,** 012309.