

NTNU  
Department of Physical Electronics

**Quantum key distribution: Real-time compensation of  
interferometer phase drift**

**Student: Alexei Brylevski**

**Supervisor: Professor Dag R. Hjelme**

**Co-supervisor: PhD student Vadim Makarov**

Abstract.....	3
1. A quick historical overview .....	4
2. Classical cryptosystems.....	5
2.1. Vernam cipher .....	5
2.2. Public key cryptography.....	6
3. Quick history of QKD .....	8
4. BB84 protocol .....	10
5. QKD setup implementations .....	12
5.1. Polarization coding.....	12
5.2. Phase coding.....	15
5.3. "Plug and Play" systems.....	20
6. Experimental setup .....	23
7. Phase adjustment in interferometer .....	28
7.1. Effect of phase error on quantum bit error rate .....	29
7.2. Phase adjustment algorithm.....	30
7.3. Obtained results .....	33
7.4. Discussion of results.....	36
Conclusion.....	39
Acknowledgements .....	40
Appendix 1 .....	41
Appendix 2 .....	42
References .....	44

## **Abstract**

Quantum key distribution (QKD) systems are described in comparison to other cryptosystems; the basic key-distribution protocol and different hardware implementations of QKD systems reviewed.

An experimental QKD setup using phase-coding scheme was assembled and tested. A technique for compensating phase drift in real time was developed, implemented and tested. Results show that such a technique will work even on single-photon level, i.e. without adding components such as variable attenuator to the system.

## 1. A quick historical overview\*

We live in the world of information. Over the last century it became obvious that nothing is as valuable as information. In the last several decades with the growth of Internet there was a big breakthrough in the field of information interchange. A huge amounts of data is being sent every day. It is obvious that valuables should be secured, so the information, too, should be transferred securely because of its value. It is especially important to provide secrecy in government, diplomatic, military and business communications. Even love letters sometimes need to be sent securely. And that's what cryptography is dealing with. From the ancient times one people tried to encrypt messages so they would be impossible to read by an unauthorized person, while other people constantly tried to crack the encrypted messages. This contest of codemakers and codebrakers is like the contest of armour and shell. And each time codemakers invented a new encryption technique, codebrakers tried to take the advantage back by inventing a new, state-of-the-art technology or algorithm that will make this technique useless against them. It was many times in history when codemakers proclaimed they have made an "uncrackable" cipher, and then after a while someone's attempt to crack this cipher was successful. For example, the most well-known case is about Enigma – the machine German military forces were using for secure communications during Second World War. Until the very end of the war germans believed that their military communications are completely secure, while actually the Enigma cipher was cracked by Polish cryptanalyst, Marian Rejewski, in the early 1930's [1]. Since that time Enigma was upgraded several times, but English codebrakers, whose knowledge was based on Rejewski achievements, were still able to read most of German communications.

---

\* Those who are familiar with cryptography in general may skip this chapter and go directly to the chapter 3.

## 2. Classical cryptosystems

All modern classical cryptosystems can be divided into two major groups: symmetrical cryptosystems and asymmetrical ones. Symmetrical, or secret-key cryptosystems are such systems, where Alice and Bob (the conventional names for the sender and receiver, respectively) share a piece of information, namely a key, which is supposed to be unknown to Eve (the conventional name given to the adversary in cryptology). The key is applied each time for encryption and decryption. In contrast, asymmetrical, or public-key cryptosystems are dealing with the pairs of keys. One of them (public key) is used for encryption, and the other one (private key) is used for decryption of messages.

### 2.1. Vernam cipher

Vernam cipher, or "one-time pad", discovered by Gilbert Vernam at AT&T in 1917 (first published in 1926), belongs to the category of symmetrical cryptosystems. In the Vernam scheme, Alice encrypts her message, a string of bits denoted by the binary number  $m_1$ , using a randomly generated key  $k$ . She simply adds each bit of the message with the corresponding bit of the key to obtain the scrambled text ( $s = m_1 \oplus k$ , where  $\oplus$  denotes the binary addition modulo 2 without carry). It is then sent to Bob, who decrypts the message by subtracting the key ( $s - k = m_1 \oplus k - k = m_1$ ). Because the bits of the scrambled text are as random as those of the key, they do not contain any information. This cryptosystem is thus provably secure in the sense of information theory (Shannon 1949). Actually, this is today the only provably secure cryptosystem. [2] The perfect security of this cryptosystem exists only on conditions that:

1. The key is completely random
2. It is as long as message itself
3. It is used only once for one single message (hence the name "one-time pad")

Reusing the key to encrypt several messages would lead to some structure in the ciphertext, and Eve could take advantage of that. For example, If Eve recorded two different messages encrypted with the same key, she could add the scrambled text to obtain the sum of the plain texts:  $s_1 \oplus s_2 = m_1 \oplus m_2 \oplus k \oplus k = m_1 \oplus m_2$ , where we used the fact that  $\oplus$  is commutative.

So, the main disadvantage of such system is necessity of having big amounts of the random key data shared securely between Alice and Bob. The keys have to be transmitted somehow, with the help of a trusted courier or through a personal meeting between Alice and Bob. Since the procedure of key delivering can be complex and expensive, there was an attempt to avoid it. This caused invention of a new, “asymmetrical” type of cryptosystems.

## 2.2. Public key cryptography

The principle of public key cryptography was proposed in 1976 by Whitfield Diffie and Martin Hellman, who were then at Stanford university in the US. The idea was to use two different keys – one key for encryption and the other one for decryption. The encryption key does not have to be hidden from potential adversary – moreover, this key is supposed to be spread as widely as possible, for any sender to be able to send messages to Bob. So, this key is called “public”. In contrast with this key, the decryption key, or “private” key, have to be held by Bob in secret, because otherwise Eve will be able to decipher the messages sent to Bob. These two keys must be connected by the means of a one-way function, which will make it easy to compute public key from the private one, but which will make extremely hard to do the reverse calculation. Although this principle was invented in 1976, no one at this time knew the one-way function to fulfill these requirements. However, in 1978 Ronald Rivest, Adi Shamir and Leonard Adleman succeeded in finding such a function, which was then implemented in an algorithm known as RSA. [1]

The security of public key cryptosystems is based on computational complexity. The idea is to use mathematical objects called one-way functions. By definition, it is easy to compute the function  $f(x)$  given the variable  $x$ , but difficult to reverse the calculation and compute  $x$  from  $f(x)$ . In the context of computational complexity, the word "difficult" means that the time to do a task grows exponentially with the number of bits in the input, while "easy" means that it grows polynomially. Intuitively, it is easy to understand that it only takes a few seconds to work out  $67 \times 71$ , but it takes much longer to find the prime factors of 4757. However, factoring has a "trapdoor", which means that it is easy to do the calculation in the difficult direction provided that you have some additional information. For example, if you were told that 67 was one of the prime factors of 4757, the calculation would be relatively simple. The security of RSA is actually based on the factorization of large integers. [2] For now, RSA cipher is considered to be secure enough for most of the applications of modern cryptography. The most popular cryptographic software known as PGP (Pretty Good Privacy) is based on RSA principle. Developed in 1991 by Phil Zimmermann, PGP shortly become very popular among Internet users. For now most of the bank transactions, e-shopping, commercial and non-commercial secure communications exploit RSA cipher.

So, public-key cryptography overcomes the main disadvantage of secret-key systems: there is no more need of secure key exchange. However, RSA cryptosystems suffer from a major flaw: whether factoring is "difficult" or not could never be proven. This implies that the existence of a fast algorithm for factorization cannot be ruled out. But this is not all. In 1985 David Deutsch described the principle of quantum computer – a computer that qualitatively differs from an ordinary one by exploiting the fundamental laws of quantum physics. This computer will have dramatically high performance compared to all possible present and future classical computers. Moreover, in 1994 Peter Shor of AT&T Bell laboratories did succeed in defining a series of steps that could be used by a quantum computer to factor a giant number [22] – just what is required to crack

the RSA cipher. Unfortunately, Shor could not demonstrate his factorization program, because there was still no such thing as quantum computer.

For now, no one knows how to make a quantum computer. But no one can prove that quantum computer cannot be built at all. Moreover, one cannot claim that a quantum computer still does not exist – it can be already built in a secret military lab and remain hidden under the veil of government secrecy. We have enough examples of such kind in cryptology. One of them is about RSA cipher. The truth is, the public-key cryptosystems were invented in 1969 by James Ellis in British GCHQ (Government Communications Headquarters). This fact was revealed only in 1997, when RSA was already spread around the world.

So, we cannot be absolutely sure in perfect secrecy of public key cryptography. Now, the only absolutely secure cryptosystem is one-time pad. Again, we are faced to the problem of secure key exchange. And this problem can successfully be solved by QKD – Quantum Key Distribution systems.

### **3. Quick history of QKD**

Quantum key distribution was invented by Charles Bennett and Gilles Brassard in 1984 [16]. The predecessor to this invention was Stephen Wiesener's concept of "quantum money" which are impossible to counterfeit [17]. Wiesener's idea was to "charge" dollar bill with several photons, polarized in two non-orthogonal bases. According to Heisenberg's uncertainty principle, there are quantum states which are incompatible in the sense that measuring one property necessarily randomizes the value of the other. So, to counterfeit a dollar bill, a counterfeiter must measure the states of all photons "trapped" in the bill, and then reproduce them in his new bill. However, he does not know the initial bases in which the photons were coded (this information is kept in secret by the bank which produces these bills), so by measuring one of the properties (to say, vertical/horizontal polarisations) of a photon he randomises the other (to say, left/right circular polarisations). It is obvious that this measurement will produce



about 50% error. But the bank knows the right bases for the each photon in the bill from the very beginning and thus it is capable of obtaining all of the information from this quantum system. It then compares the measured data with the data recorded in its database and makes a decision whether the bill was counterfeited or not [1]. The idea of quantum money was brilliant, but it was also wholly impractical: it is impossible to store a photon trapped for a sufficiently long period of time. That's why Wiesener's article about quantum money was rejected in several scientific journals.

However, Bennett and Brassard thought of it in other way: rather to store information, polarized photons can transmit it through a quantum channel. As a rule, this quantum channel is represented by an optical fiber – an ordinary singlemode fiber often used in classical data transmission systems. The transmission is done by a light pulses which are so weak that the probability of a photon appearing in each of the light pulses is considerably lower than 1 photon per pulse. The plot of the entire QKD system is to provide Alice and Bob with an identical sequence of random bits, which then can be used as a key to encrypt messages via one-time pad technique.

## 4. BB84 protocol

The basic quantum key distribution protocol begins with Alice sending a random sequence of the four canonical kinds of polarized photons to Bob. Bob then chooses randomly and independently for each photon (and independently of the choices made by Alice, since these choices are unknown to him at this point) whether to measure the photon's rectilinear or circular polarization (figure 1). Bob then announces publicly which kind of measurement he made (but not the result of the measurement), and Alice tells him, again publicly, whether he made the correct measurement (i.e., rectilinear or circular). Alice and Bob then agree publicly to discard all bit positions for which Bob performed the wrong measurement. Similarly, they agree to discard bit positions where Bob's detectors failed to detect the photon at all. The polarizations of the remaining photons is interpreted as bit 0 for horizontal or left-circular, and bit 1 for vertical and right-circular. The resulting binary string should be shared secret information between Alice and Bob, provided that no eavesdropping on the quantum channel has taken place. The result of the above steps is referred to as the raw quantum transmission. [3]

1.	↻	↑	↺	↔	↓	↓	↔	↔	↺	↻	↑	↺	↻	↻	↓
2.	+	○	○	+	+	○	○	+	○	+	○	○	○	○	+
3.	↓		↺		↓	↻	↻	↔		↓	↺	↺		↻	↓
4.	+		○		+	○	○	+		+	○	○		○	+
5.			✓		✓			✓				✓		✓	✓
6.			↺		↓			↔				↺		↻	↓
7.			1		1			0				1		0	1

Fig. 1. Illustration of basic quantum key distribution protocol.

1. Alice sends a random sequence of photons polarized horizontal, vertical, right-circular and left-circular;
2. Bob measures the photons' polarization in a random sequence of bases, rectilinear and circular;

3. Results of Bob's measurements (some photons may not be received at all);
4. Bob tells Alice which basis he used for each photon he received;
5. Alice tells him which bases were correct;
6. Alice and Bob keep only the data from these correctly-measured photons, discarding all the rest;
7. This data is interpreted as a binary sequence according to the coding scheme (horizontal = left-circular = 0 and vertical = right-circular = 1).

In the basic protocol, Alice and Bob next test for eavesdropping by publicly comparing polarizations of a random subset of the photons on which they think they should agree. No measurement the eavesdropper can make on one of these photons while it is in transit from Alice to Bob can yield more than  $1/2$  expected bit of information on its polarization. If Alice and Bob find no discrepancies, and if it is safe to assume that Eve cannot corrupt the contents of the public messages exchanged between them, then Alice and Bob may safely conclude that there are few or no errors in the remaining uncomparing data, and that little or none of it is known to any eavesdropper.

Actually, more complicated computations have to be made with the raw key to make it usable and check for eavesdropping. Realistic detectors have some noise; therefore, Alice's and Bob's data will differ even in the absence of eavesdropping. Accordingly, an error correction protocol have to be implemented.

Once the quantum transmission has been completed, the first task is for Alice and Bob to exchange public messages enabling them to reconcile the differences between their data. Because we assume that Eve listens to all the public messages between Bob and Alice, this exchange must be performed in a way that reveals as little information as possible on this data. An effective way for Alice and Bob to perform reconciliation is for them first to make a random permutation of the bit positions in their strings, to randomize the locations of errors, then partition the permuted strings into blocks of size  $k$  such that single blocks

are believed to be unlikely to contain more than one error. For each such block, Alice and Bob compare the block's parity. Blocks with matching parity are accepted as correct, while those of discordant parity are dividing to several sub-blocks, and parity check is performing on each subblock, until the error is found and corrected. If the initial block size was much too large or too small, due to a bad initial guess of the error rate, that fact will become apparent, and the procedure can be repeated with a more suitable block size. In order to avoid leaking information to Eve during the reconciliation process, Alice and Bob agree to discard the last bit of each block or subblock whose parity they have disclosed. Even with an appropriate block size, some errors will typically remain undetected, having occurred in blocks or subblocks with an even number of errors [3]. To remove additional errors, the random permutation and block parity disclosure is repeated several more times, with increasing block sizes, until Alice and Bob estimate that at most a few errors remain in the data as a whole. At some point, all errors will have been removed, but Alice and Bob will not yet be aware of their success. After the last detected error, Alice and Bob continue comparing parities until sufficiently many consecutive agreements (say 20) have been found to assure them that their strings are indeed identical, with a negligible probability of not detecting the existence of remaining errors.

## **5. QKD setup implementations**

There are several possible types of QKD setups. The two main types are based on polarization coding and phase coding.

### **5.1. Polarization coding**

A typical system for quantum cryptography with the BB84 four states protocol using the polarization of photons is shown in Fig. 2.

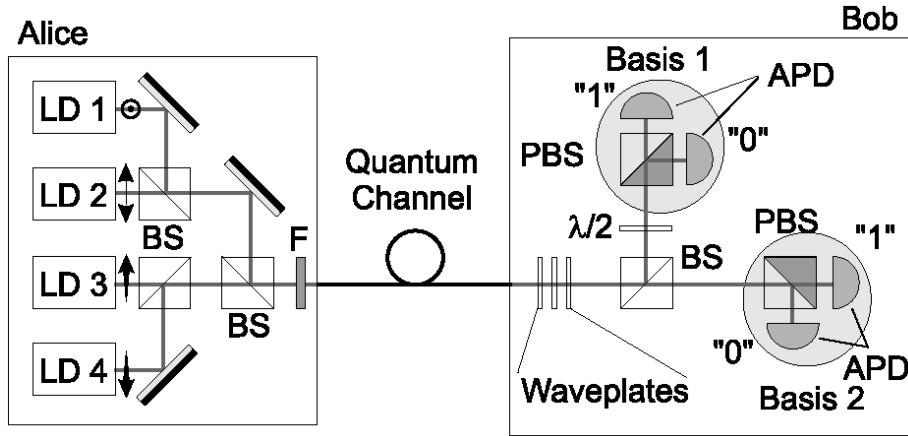


Fig. 2. Typical system for quantum cryptography using polarization coding (LD: laser diode, BS: beamsplitter, F: neutral density filter, PBS: polarizing beam splitter,  $\lambda/2$ : half waveplate, APD: avalanche photodiode).

Alice's system consists of four laser diodes. They emit short classical photon pulses (1 ns) polarized at  $-45^\circ$ ,  $0^\circ$ ,  $+45^\circ$ , and  $90^\circ$ . For bit transmission, a single diode is triggered. The pulses are then attenuated by a set of filters to reduce the average number of photons well below 1. They are finally injected into an optical fiber and leave Alice's. It is essential that the pulses remain polarized for Bob to be able to extract the information encoded by Alice. [2]

Polarization mode dispersion may depolarize the photons, provided the delay it introduces between both polarization modes is larger than the coherence time. This sets a constraint on the type of lasers used by Alice. When reaching Bob, the pulses are extracted from the fiber. They travel through a set of waveplates used to recover the initial polarization states by compensating the transformation induced by the optical fiber. The pulses reach then a symmetric beam splitter, implementing the basis choice. Transmitted photons are analyzed in the vertical-horizontal basis with a polarizing beamsplitter and two photon counting detectors. The polarization state of the reflected photons is first rotated with a waveplate by  $45^\circ$  ( $-45^\circ$  to  $0^\circ$ ). The photons are then analyzed with a second set of polarizing beamsplitter and photon counting detectors. This implements the diagonal basis. For illustration, let us follow a photon polarized at  $+45^\circ$ , we see

that its state of polarization is arbitrarily transformed in the optical fiber. At Bob's end, the polarization controller must be set to bring it back to  $+45^\circ$ . If it chooses the output of the beamsplitter corresponding to the vertical-horizontal basis, it will experience equal reflection and transmission probability at the polarizing beamsplitter, yielding a random outcome. On the other hand, if it chooses the diagonal basis, its state will be rotated to  $90^\circ$ . The polarizing beamsplitter will then reflect it with unit probability, yielding a deterministic outcome. Instead of Alice using four lasers and Bob two polarizing beamsplitters, it is also possible to implement this system with active polarization modulators such as Pockels cells [4]. For emission, the modulator is randomly activated for each pulse to rotate the state of polarization to one of the four states, while, at the receiver, it randomly rotates half of the incoming pulses by  $45^\circ$ .

Antoine Muller and his coworkers at the University of Geneva used such a system to perform QC experiments over optical fibers [9]. They created a key over a distance of 1100 meters with photons at 800 nm. In order to increase the transmission distance, they repeated the experiment with photons at 1300nm [10], [11] and created a key over a distance of 23 kilometers. An interesting feature of this experiment is that the quantum channel connecting Alice and Bob consisted in an optical fiber part of an installed cable, used by the telecommunication company Swisscom for carrying phone conversations. This was the first time QC was performed outside of a physics laboratory.

These two experiments highlighted the fact that the polarization transformation induced by a long optical fiber was unstable over time. Indeed, Muller noticed that, although it remained stable and low for some time (of the order of several minutes), it would suddenly increase after a while, indicating a modification of the polarization transformation in the fiber. This implies that a real QC system requires active alignment to compensate for this evolution. Although not impossible, such a procedure is certainly difficult. James Franson did indeed implement an active feedback alignment system [12], but did not pursue along this direction. There are more choices for active polarization control developed

for coherent fiber-optic communication systems [18]. It is interesting to note that replacing standard fibers with polarization maintaining fibers does not solve the problem. The reason is that, in spite of their name, these fibers do not maintain polarization. Because of this problem, polarization coding does not seem to be the best choice for QC in optical fibers. Nevertheless, the situation is drastically different when considering free space key exchange, as the air has essentially no birefringence at all.

## 5.2. Phase coding

The polarization drift in polarization coding based QKD setups makes them very difficult (although not impossible) to implement. In search of the solution, scientists have devised another basic QKD setup scheme. The idea of encoding the value of bits in the phase of photons was first mentioned by Bennett in the paper where he introduced the two-states protocol [3]. It is indeed a very natural choice for optics specialists. State preparation and analysis are then performed with interferometers, that can be realized with single-mode optical fibers components [2]. Fig. 3 presents an optical fiber version of a Mach-Zehnder interferometer.

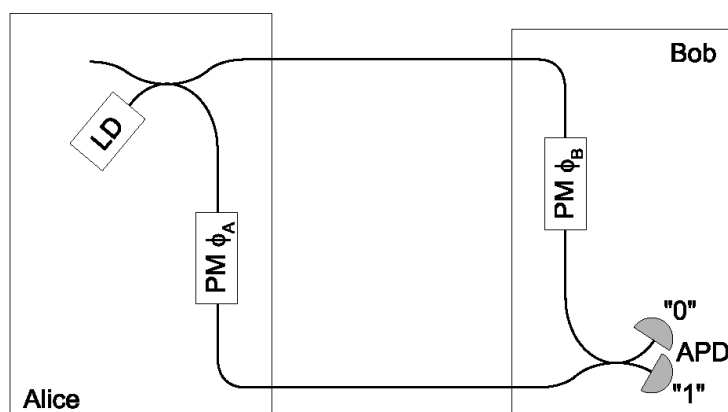


Fig. 3. Mach-Zehnder interferometer.

It is made out of two symmetric couplers - the equivalent of beamsplitters - connected to each other, with one phase modulator in each arm. One can

inject light in the set-up using a continuous and classical source, and monitor the intensity at the output ports. Provided that the coherence length of the light used is larger than the path mismatch in the interferometers, interference fringes can be recorded. Taking into account the  $\pi/2$  phase shift experienced upon reflection at a beamsplitter, the effect of the phase modulators ( $\varphi_A$  and  $\varphi_B$ ) and the path length difference ( $\Delta L$ ), the intensity in the output port labeled "0" is given by:

$$I_0 = \bar{I} \cdot \cos^2\left(\frac{\varphi_A - \varphi_B + k\Delta L}{2}\right),$$

where  $k$  is the wave number and  $I$  the intensity of the source. If the phase term is equal to  $\pi/2 + n\pi$ , where  $n$  is an integer, destructive interference is obtained. Therefore the intensity registered in port "0" reaches a minimum and all the light exits in port "1". When the phase term is equal to  $n\pi$ , the situation is reversed: constructive interference is obtained in port "0", while the intensity in port "1" goes to a minimum. With intermediate phase settings, light can be recorded in both ports. This device acts like an optical switch. It is essential to keep the path difference stable in order to record stationary interferences.

Although we discussed the behavior of this interferometer for classical light, it works exactly the same when a single photon is injected. The probability to detect the photon in one output port can be varied by changing the phase. Although a photon behaves as a particle on detection it propagates through the interferometer as a wave. [6] The Mach-Zehnder interferometer is the fiber optic version of Young's slits experiment, where the arms of the interferometer replace the apertures. This interferometer combined with a single photon source and photon counting detectors can be used for quantum key distribution. Alice's setup consists of the source, the first coupler and the first phase modulator, while Bob takes the second modulator and coupler, as well as the detectors. Let us consider the implementation of the four-states BB84 protocol. On the one hand, Alice can apply one of four phase shifts ( $0, \pi/2, \pi, 3\pi/2$ ) to encode a bit value. She associates  $0$  and  $\pi/2$  to bit  $0$ , and  $3\pi/2$  to bit  $1$ . On the other hand, Bob performs a basis choice by applying randomly a phase shift of either  $0$  or



$\pi/2$ , and he associates the detector connected to the output port "0" to a bit value of 0, and the detector connected to the port "1" to 1. When the difference of their phase is equal to 0 or  $\pi$ , Alice and Bob are using compatible bases and they obtain deterministic results. In such cases, Alice can infer from the phase shift she applied, the output port chosen by the photon at Bob's end and hence the bit value he registered. Bob, on his side, deduces from the output port chosen by the photon, the phase that Alice selected. When the phase difference equals  $\pi/2$  or  $3\pi/2$ , they use incompatible bases and the photon chooses randomly which port it takes at Bob's coupler. All possible combinations are summarized in Table 1.

Alice		Bob		
Bit value	$\varphi_A$	$\varphi_B$	$\varphi_A - \varphi_B$	Bit value
0	0	0	0	0
0	0	$\pi/2$	$3\pi/2$	?
1	$\pi$	0	$\pi$	1
1	$\pi$	$\pi/2$	$\pi/2$	?
0	$\pi/2$	0	$\pi/2$	?
0	$\pi/2$	$\pi/2$	0	0
1	$3\pi/2$	0	$3\pi/2$	?
1	$3\pi/2$	$\pi/2$	$\pi$	1

Table 1: Implementation of the BB84 four-states protocol with phase encoding.

It is essential with this scheme to keep the path difference stable during a key exchange session. It should not change by more than a fraction of a wavelength of the photons. A drift of the length of one arm would indeed change the phase relation between Alice and Bob, and induce errors in their bit sequence. Although this scheme works perfectly well on an optical table, it is impossible to keep the path difference stable when Alice and Bob are separated by more than a few meters. The relative length of the arms should not change by more than a fraction of a wavelength. Considering a separation between Alice and Bob of 1

kilometer for example, it is clear that it is not possible to prevent path difference changes smaller than  $1\mu\text{m}$  caused by environmental variations. Bennett showed how to get round this problem [3]. He suggested to use two unbalanced Mach-Zehnder interferometers connected in series by a single optical fiber (see Fig. 4), both Alice and Bob being equipped with one.

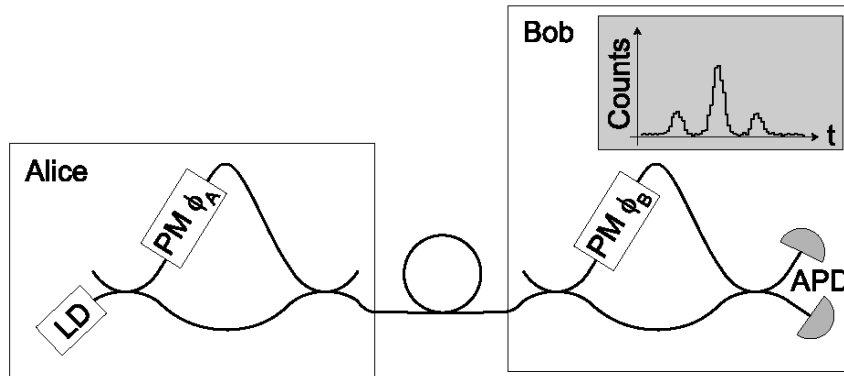


Fig. 4. Double Mach-Zehnder implementation of an interferometric system for quantum cryptography (LD: laser diode, PM: phase modulator, APD: avalanche photodiode).

When monitoring counts as a function of the time since the emission of the photons, Bob obtains three peaks. The first one corresponds to the cases where the photons chose the short path both in Alice's and in Bob's interferometers, while the last one corresponds to photons taking twice the long paths. Finally, the central peak corresponds to photons choosing the short path in Alice's interferometer and the long one in Bob's, and to the opposite. If these two processes are indistinguishable, they produce interference. A timing window can be used to discriminate between interfering and non-interfering events. Disregarding the latter, it is then possible for Alice and Bob to exchange a key.

The advantage of this set-up is that both "halves" of the photon travel in the same optical fiber. [2] They experience thus the same optical length in the environmentally sensitive part of the system, provided that the variations in the fiber are slower than their temporal separations, determined by the interferome-

ter's imbalance ( $\approx 5\text{ns}$  in Bennett's setup). This condition is much less difficult to fulfill. In order to obtain a good interference visibility, and hence a low error rate, the imbalances of the interferometers must be equal within a fraction of the coherence time of the photons. This implies that the path differences must be matched within a few millimeters, which does not constitute a problem. Besides, the imbalance must be chosen so that it is possible to clearly distinguish the three temporal peaks and thus discriminate interfering from non-interfering events. It must then typically be larger than the pulse length and than the timing jitter of the photon counting detectors. In practice, the second condition is the most stringent one. Assuming a time jitter of the order of  $500\text{ps}$ , an imbalance of at least  $1.5\text{ns}$  keeps the overlap between the peaks low.

The main difficulty associated with this scheme is that the imbalances of Alice's and Bob's interferometers must be kept stable within a fraction of the wavelength of the photons during a key exchange to maintain correct phase relations. [8] This implies that the interferometers must lie in containers whose temperature is stabilized. In addition, for long key exchanges an active system is necessary to compensate the drifts. Finally, in order to ensure the indistinguishability of both interfering processes, one must make sure that in each interferometer the polarization transformation induced by the short path is the same as the one induced by the long one. Alice as much as Bob must then use a polarization controller. However, the polarization transformation in short optical fibers whose temperature is kept stable, and which do not experience strains, is rather stable. This adjustment does thus not need to be repeated frequently.

Paul Tapster and John Rarity from DERA working with Paul Townsend were the first ones to test this system over a fiber optic spool of 10 kilometers in 1993 [19]. Townsend later improved the interferometer by replacing Bob's input coupler by a polarization splitter to suppress the lateral non-interfering peaks [13]. In this case, it is unfortunately again necessary to align the polarization state of the photons at Bob's, in addition to the stabilization of the interferome-

ters imbalance. He later thoroughly investigated key exchange with phase coding and improved the transmission distance [5, 14]. He also tested the possibility to multiplex at two different wavelengths a quantum channel with conventional data transmission over a single optical fiber [15]. Richard Hughes and his co-workers from Los Alamos National Laboratory also extensively tested such an interferometer [7].

### 5.3. "Plug and Play" systems

In systems described above an active compensation technique has to be implemented to compensate for quantum channel characteristics fluctuations. An approach invented in 1989 by Martinelli, then at CISE Tecnologie Innovative in Milano, allows to automatically and passively compensate all polarization fluctuations in an optical fiber [21]. The schematic is shown on Fig. 5.

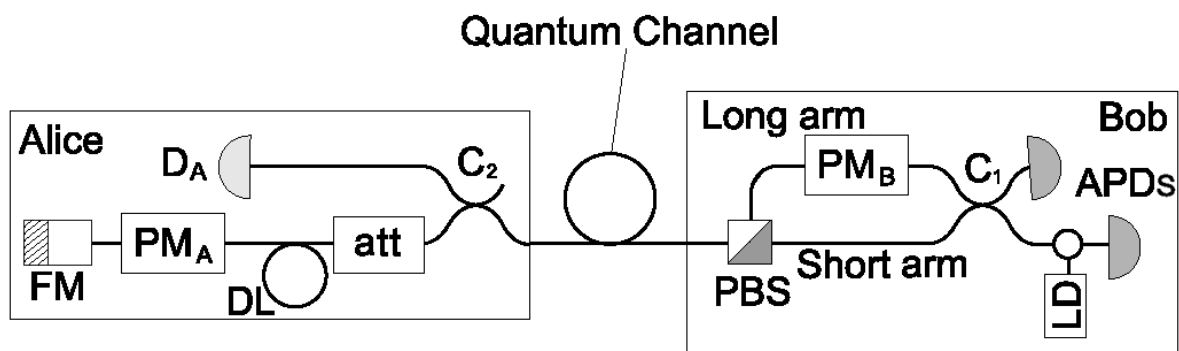


Fig. 5. "Plug and Play" system (LD: laser diode, APD: avalanche photodiode, C - fiber coupler, PM - phase modulator, PBS: polarizing beamsplitter, DL - optical delay line, FM - Faraday mirror, D<sub>A</sub>- classical detector, att – optical attenuator).

In this scheme, pulses emitted at Bob can travel either via the short arm at Bob, be reflected at the Faraday mirror FM at Alice's and finally, back at Bob, travel via the long arm. Or, they travel first via the long arm at Bob, get reflected at Alice, travel via the short arm at Bob and then superpose on beamsplitter C<sub>1</sub>

[2]. We now explain the realization of this scheme more in detail: A short and bright laser pulse is injected in the system through a circulator. It splits at a coupler. One of the half pulses, labeled  $P_1$ , propagates through the short arm of Bob's set-up directly to a polarizing beamsplitter. The polarization transformation in this arm is set so that it is fully transmitted.  $P_1$  is then sent onto the fiber optic link. The second half pulse, labeled  $P_2$ , takes the long arm to the polarizing beamsplitter. The polarization evolution is such that it is reflected into the line. A phase modulator present in this long arm is left inactive so that it imparts no phase shift to the outgoing pulse.  $P_2$  is also sent onto the link, with a delay of the order of 200 ns. Both half pulses travel to Alice.  $P_1$  goes through a coupler. The diverted light is detected with a classical detector to provide a timing signal. The non-diverted light propagates then through an attenuator and an optical delay line - consisting simply of an optical fiber spool - whose role will be explained later. Finally it passes a phase modulator, before being reflected by Faraday mirror.  $P_2$  follows the same path. Alice activates briefly her modulator to apply a phase shift on  $P_1$  only, in order to encode a bit value exactly like in the traditional phase coding scheme. The attenuator is set so that when the pulses leave Alice, they do not contain more than a fraction of a photon. When they reach the PBS after their return trip through the link, the polarization state of the pulses is exactly orthogonal to what it was when they left, thanks to the effect of the Faraday mirror.  $P_1$  is then reflected instead of being transmitted. It takes the long arm to the coupler. When it passes, Bob activates his modulator to apply a phase shift used to implement the basis choice. Similarly,  $P_2$  is transmitted and takes the short arm. Both pulses reach the coupler at the same time and they interfere. Single-photon detectors are then used to record the output port chosen by the photon.

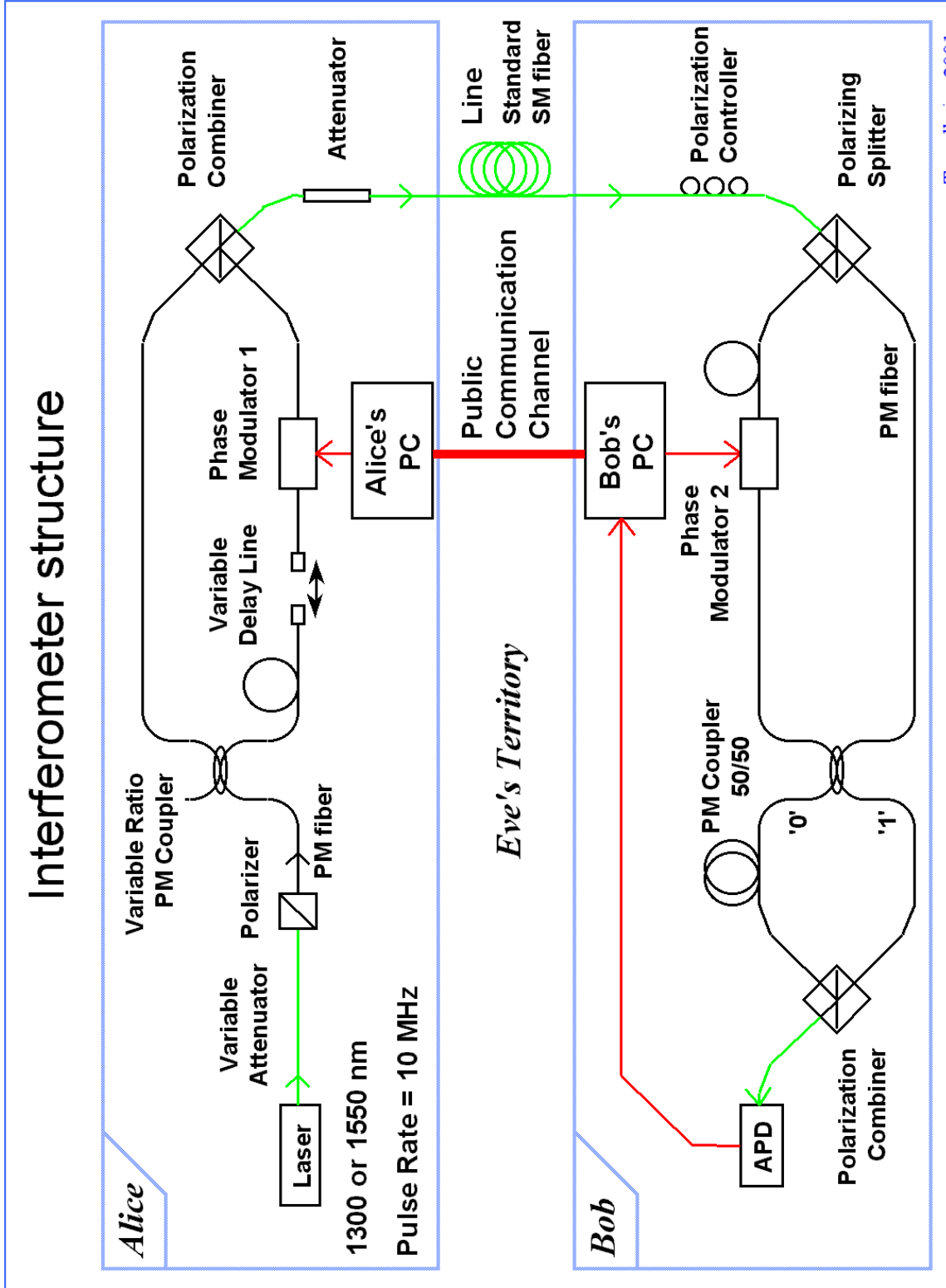
Because of the intrinsically bi-directional nature of this system, great attention must be paid to Rayleigh backscattering. The light traveling in an optical fiber undergoes scattering by inhomogeneities. A small fraction (1%) of this light is recaptured by the fiber in the backward direction. When the repetition

rate is high enough, pulses traveling to Alice and back from her intersect at some point along the line. Their intensity is however strongly different. The pulses are more than a thousand times brighter before than after reflection from Alice. Backscattered photons can accompany a quantum pulse propagating back to Bob and induce false counts. This problem have to be avoided by making sure that pulses traveling from and to Bob are not present in the line simultaneously. They are emitted in the form of trains by Bob. Alice stores these trains in her optical delay line, which consists of an optical fiber spool. Bob waits until all the pulses of a train have reached him, before sending the next one. Although it completely solves the problem of Rayleigh backscattering induced errors, this configuration has the disadvantage of reducing the effective repetition frequency. A storage line half long as the transmission line amounts to a reduction of the bit rate by a factor of approximately three. The main disadvantage of "Plug and Play" systems with respect to the other systems is that they are more sensitive to Trojan horse strategies [20]. Indeed, Eve could send a probe beam and recover it through the strong reflection by the mirror at the end of Alice's system. To prevent such an attack, Alice adds an attenuator to reduce the amount of light propagating through her system. In addition, she must monitor the incoming intensity using a classical linear detector. Besides, "plug & play" systems cannot be operated with a true single-photon source, and will thus not benefit from the progress in this field. Indeed, the fact that the pulses travel along a round trip implies that losses are doubled, yielding a reduced counting rate.

## 6. Experimental setup

The experimental setup we use utilizes the phase coding scheme and BB84 protocol. We can divide it into two main parts: optical part and electronic one. The optical part, which is a Mach-Zehnder interferometer, is represented on figure 6.

Light pulse is emitted by 1300nm semiconductor laser (Fujitsu FLD3F6CX). It passes through a polarizer, enters into polarization-maintaining fiber and then splits on variable coupler into two arms. In one of the arms it passes through Alice's phase modulator which applies certain phase shift to the pulse. This arm also includes a variable delay line for fine adjustment of the length difference between interferometer's arms, which should be close to zero. Pulses then pass Alice's polarization combiner and travel through the transmission line consisting of standard singlemode fiber. At Bob, light pulses pass through a polarization controller which is needed to compensate for static polarization transformation the pulses undergo in the transmission line. Then pulses split on Bob's polarizing splitter, such that the pulse that travelled the long arm at Alice goes into the short arm at Bob, and the one that travelled the short arm at Alice goes into the long arm at Bob where it becomes phase-shifted by Bob's phase modulator. Finally, pulses interfere on Bob's coupler. The outcome of interference depends on the relative phase of the pulses, which is controlled by Alice's and Bob's phase modulators, and represents transmission of 0 and 1 in the protocol. "Zeros" and "ones" go to different outputs of the coupler. Instead of having two detectors to detect them, we delay "zeros". So, the light pulses corresponding to "zeros" and "ones" go to the same APD after passing the polarization combiner, but they reach the APD at different times.



Trondheim 2001

Fig. 6. Optical part of QKD setup



We dedicate them two time slots: during the first one only "ones" reach APD and become detected, and during the second time slot "zeros" are detected. The main clock frequency we use is 20 MHz, which means the APD is gated at this rate. If we used two separate detectors, they could be gated at 10 MHz.

The APD (Russian-made FD312L, liquid-nitrogen cooled) works in so-called Geiger mode. In this mode the APD bias is kept slightly below the breakdown voltage most of the time, so no avalanche can occur in the APD. When synchronization signal arrives, the gate pulse is added to the bias voltage, rising the voltage on APD above the breakdown level. During this gate pulse, photon detection is possible, and a photon arriving to APD can trigger an avalanche. This mode of APD operation dramatically decreases dark count rates, because most of the time, without the gate pulse, no avalanche is possible. However, synchronization requirements are strict, because the gate pulse must be applied to APD exactly at the same time as the photon is expected to arrive. We keep the pulse just wide enough (1-2 ns) to observe photon counts reliably. The longer the pulse, the higher dark count rates we will get. Our experiments show low dark count probability (about  $1E-4$ ) which is enough for QKD applications over moderate distances and can be improved by getting a better APD.

The arms of the interferometer are made of polarization-maintaining fiber (Fujikura Panda PM 1300 nm), while fibers between laser and Alice's polarizer and also between Bob's polarization combiner and detector (and of course the transmission line itself) don't have to be polarization-maintaining.

The electronic part of the setup is shown on fig. 7.

QKD setup: electrical interconnections diagram

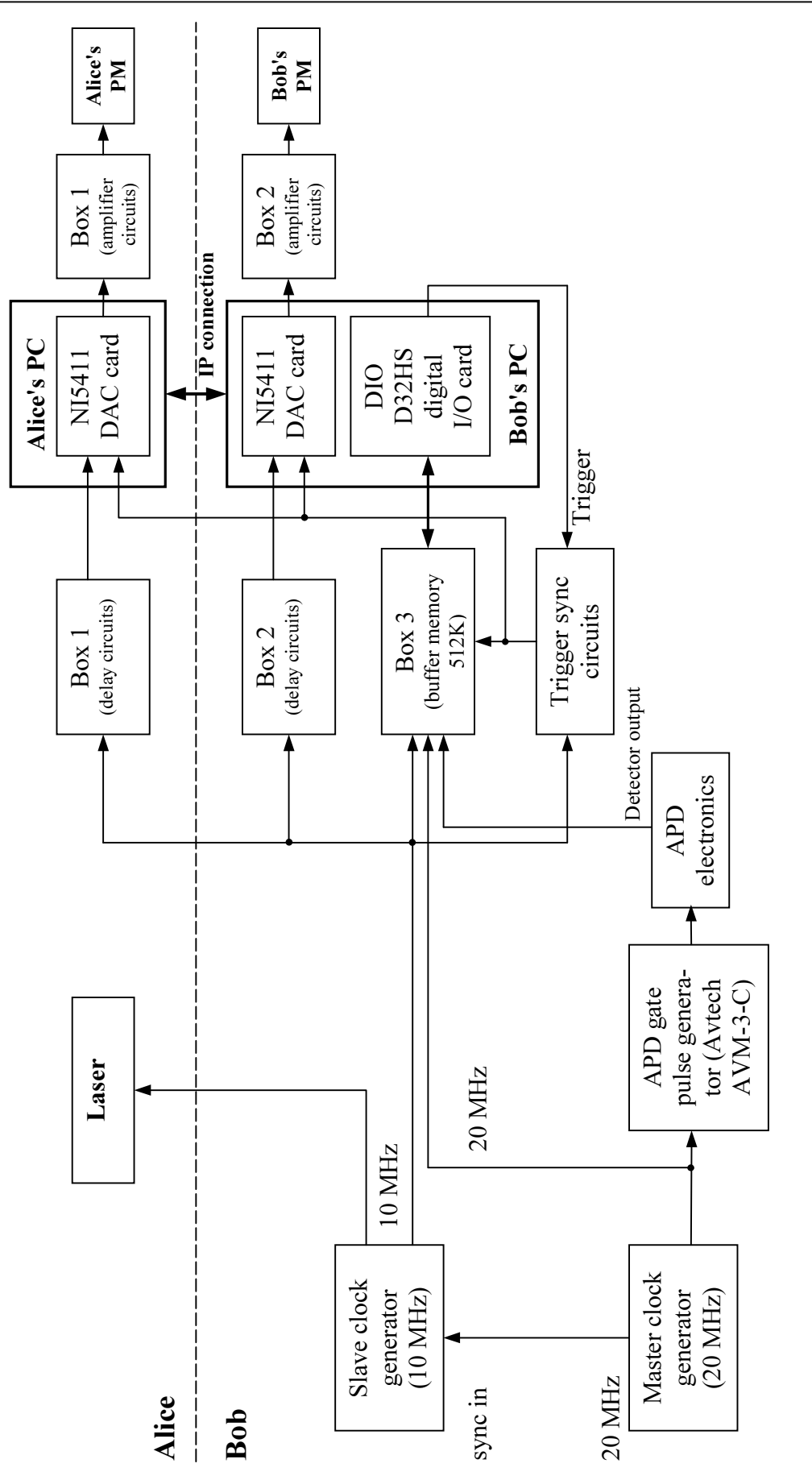


Fig. 7. Electronic setup layout

We have two PCs named Alice and Bob, which are connected via Internet (10 Mbps LAN) used as a public channel. Both Alice and Bob have National Instruments NI 5411 cards which are high-speed arbitrary waveform generators for driving their phase modulators; Bob also have DIO D32HS digital I/O card which is used for detector data acquisition. One of the outputs of this card is also used for generating trigger signal, which starts packet transmission in the whole system. Because NI 5411 cards have maximum output voltage of  $\pm 5$  V, and our phase modulators have half-wave voltage of 8.3 V, there has been made two amplifiers placed in Box1 and Box2 (for Alice and Bob respectively). These boxes also contain adjustable phase shift circuits that help to synchronize the cards. The data acquisition from APD is done by Box3, which contains digital circuits and 512KB buffer memory with 20 MHz serial input to store APD data before loading it into Bob's PC. This is made because general-purpose PCs cannot process this data in real time. The detector data is collected to the memory of Box3 and then Bob's PC reads its contents byte-by-byte using DIO D32HS card. Real-time data processing would be possible with a dedicated controller.

The whole system is synchronized from 20 MHz master clock generator (SRS DS345). Its frequency is digitally synthesized and we can consider it to be stable enough. The master clock generator synchronises slave clock generator, which is 10 MHz (HP 8008A), the generator which produces gate pulses for APD, and also Box3, which uses it for synchronization during data acquisition. The 10 MHz clock is sent to laser electronics, to Box3 (to distinguish between 0 and 1 time slots), to Box 1 and 2 (it then becomes phase-shifted according to the delay circuits settings and synchronizes the NI 5411 cards).

We had to go through quite a lot of trouble to properly synchronize the NI 5411 cards. They have two inputs - for external clock, and for external trigger. 10 MHz external clock is needed to phase-lock card's internal clocks, while trigger is a static TTL signal sent by Bob's digital I/O card to start generation of the waveform loaded into the card memory, and thus the quantum key transmission

routine. The cards were not able to lock in the absolute phase, and the timing of generated waveforms was changing from run to run. The problem was solved by tying the trigger signal to the nearest edge of the 10 MHz signal. Actually, according to the (poorly written) cards' manual, they were not supposed to work from an external trigger signal. In our case they worked, but the resulting waveform had four times higher sample rate (40 MHz) than expected. We repeated PM voltage for each bit slot four times in the pre-loaded waveform, and the problem finally seemed to be gone.

## **7. Phase adjustment in interferometer**

The error rate in raw key of QKD system depends on the accuracy of setting phase of light pulse. There are two sources of phase inaccuracy: error in setting PM voltages and phase mismatch between the two arms of interferometer. We assume that the error in the voltage values that Alice and Bob are applying to their phase modulators can be easily minimized. The problem, however, is phase drift in the interferometer. Experiments show that the relative phase between the two arms of interferometer is drifting slowly (with the speed of about  $360^\circ$  per several minutes [5]), and measurements on our own setup have confirmed that. To get our QKD system working properly we must adjust the phase before each cycle of transmission to compensate this drift.

## 7.1. Effect of phase error on quantum bit error rate

For now we assume that all possible errors in raw key are due to inaccuracy of phase settings, which means we assume there is no other sources of errors. As we know, the maximum error probability the key extraction algorithm can handle is 11%. We now determine the phase setting accuracy for this value.

If we step  $\Delta\varphi$  from the actual phase position, then instead of getting 0 and  $N_{\max}$  counts in "0" and "1" time slots we will get some A and B values. Obviously, the error probability P will be:

$$P = \frac{A}{B} = \frac{\sin^2\left(\frac{\Delta\varphi}{360^\circ}\pi\right)}{\sin^2\left(\frac{\Delta\varphi + 180^\circ}{360^\circ}\pi\right)}$$

This gives the following dependence of  $P(\Delta\varphi)$ :

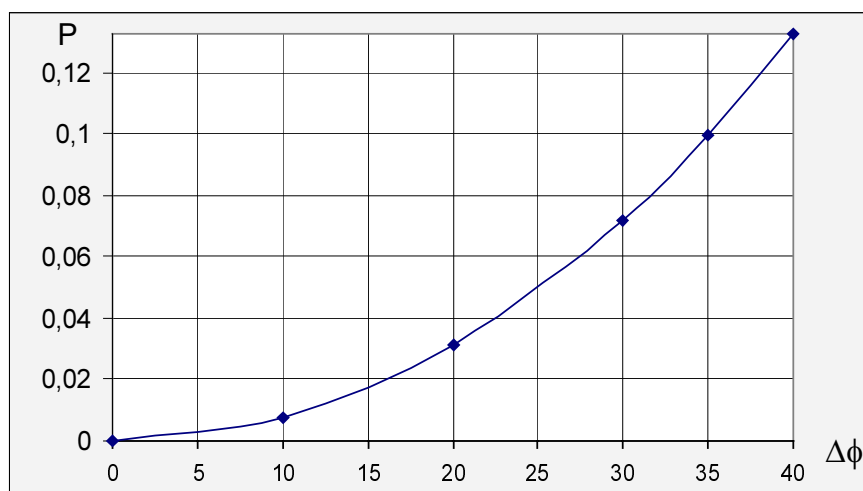


Fig. 8. Key bit error probability versus phase setting inaccuracy in degrees

As we see, to keep the error probability below 11%, the phase inaccuracy have to be below 35°.

## 7.2. Phase adjustment algorithm

There are two possibilities: manual adjustment and automatic one. In this case, manual phase adjustment will be useless even in the experiment, because the phase is drifting too fast for an operator to do appropriate changes, so we have to choose automatic. Our goal was to implement a phase adjustment technique, which will work on single-photon level, because it will not require us to use additional components such as variable attenuator. Such attenuator may be helpful in case we decide to perform phase adjustment with classical light pulses, but adding more components make the whole system more expensive and less reliable.

The algorithm we devised consists of two stages:

### **Stage 1:** Rough phase compensation

Alice sets her phase modulator in "1" state (0V) and transmits photons as usual. Bob sets his phase modulator voltage to scan the  $0^\circ$  to  $360^\circ$  range of phase in a small number of steps (say, 20). During each step he is counting the number of photons in both "0" and "1" detector time slots. In one of the steps there will be a minimum number of photons counted in "0" time slot and a maximum one counted in "1" time slot. We call the phase compensation of this step as "roughly determined phase compensation",  $\varphi_0$ .

The dependence of number of photons detected in each time slot from  $\varphi$  is shown on figure 9:

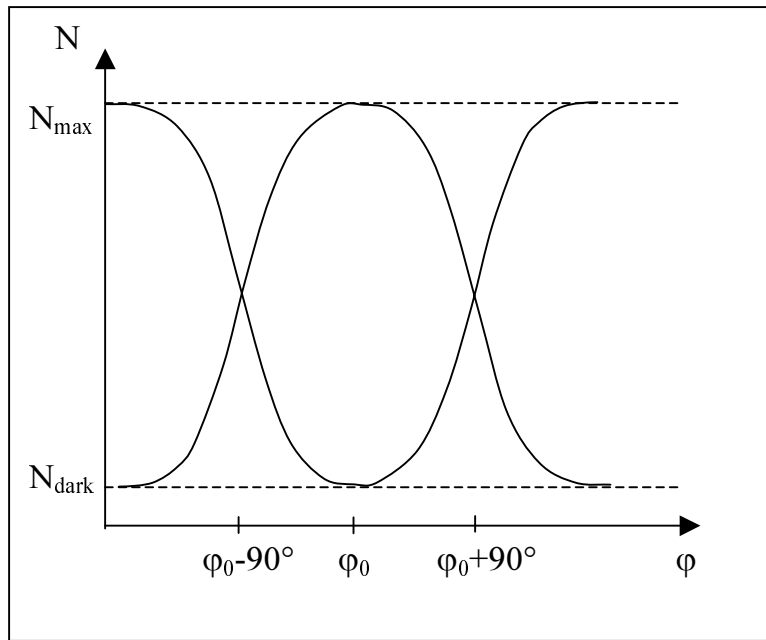


Fig. 9.  $\varphi$  - phase,  $N$  - the number of counts detected during some fixed period of time.

The minimum number of counts is limited by the number of dark counts,  $N_{\text{dark}}$ , while the maximum number of counts is  $N_{\text{max}}$ .

As we see, if Bob scans his phase in the range of  $0^\circ \dots 360^\circ$ , he will be for sure near one of the maxima of  $N_1(\varphi)$  and of one of the appropriate minima of  $N_0(\varphi)$  in one of his steps. This won't, however, give us needed accuracy of several degrees, because even if Bob will divide  $360^\circ$  interval on 360 steps, due to statistical fluctuations in  $N$  it will take too much time for Bob to count  $N$  in each of 360 steps with required precision. During this time the phase drift will take place, and we will get outdated results. To get as much accuracy as possible in a given counting time, we will have to count photons at the points on these curves where they have the maximum slope to statistical deviation ratio. To the first approximation, these points are  $\varphi_0 + 90^\circ$  and  $\varphi_0 - 90^\circ$ .

The purpose of stage 1 was to quickly provide a rough estimate of these points, and then to continue counting with the required accuracy on stage 2.

**Stage 2:** Fine phase compensation.

Alice continues sending her photons with her phase modulator in "1" state (0V), while Bob sets his modulator to  $\varphi_0+90^\circ$  and  $\varphi_0-90^\circ$  states (by alternating pattern) and finally gets four values – the numbers of photons detected with phase modulator in  $\varphi_0+90^\circ$  and  $\varphi_0-90^\circ$  states in both "1" and "0" time slots.

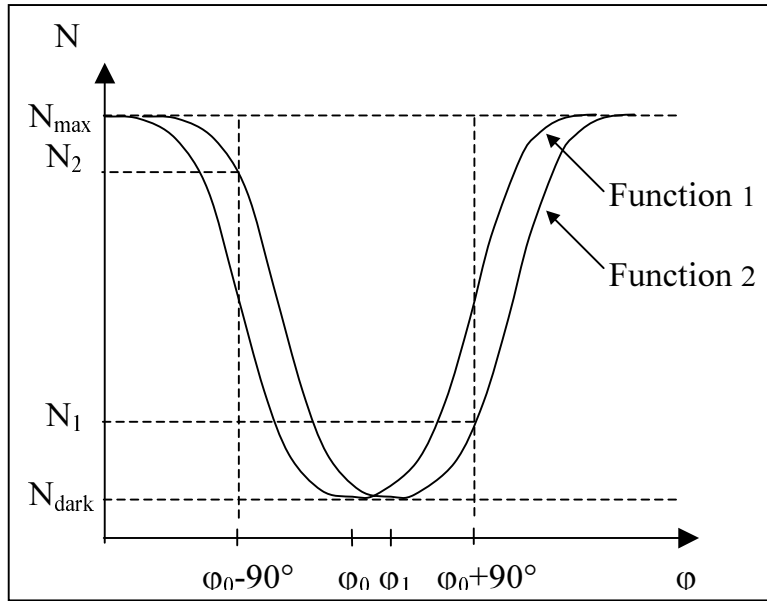


Fig. 10. Phase adjustment, step2.

On figure 10, Function 1 is our assumption of dependence  $N(\varphi)$  after performing the first stage of phase adjustment. Function 2 is the real dependence  $N(\varphi)$ , which is unknown to us at this point.

$$\text{Function 1: } N = (N_{\max} - N_{\text{dark}}) \sin^2\left(\frac{\varphi - \varphi_0}{360^\circ} \pi\right) + N_{\text{dark}}$$

$$\text{Function 2: } N = (N_{\max} - N_{\text{dark}}) \sin^2\left(\frac{\varphi - \Delta\varphi - \varphi_0}{360^\circ} \pi\right) + N_{\text{dark}}$$

$$\Delta\varphi = \varphi_1 - \varphi_0$$

$N_{\text{dark}}$  can be either 0 or value measured on stage 1

$N_{\max}$  can be either  $N_1 + N_2$  or value measured on stage 1



$$\Delta\varphi = \frac{45^\circ}{\pi} \left( \arccos\left(2 \frac{N_{dark} - N_1}{N_{max} - N_{dark}} + 1\right) - \arccos\left(2 \frac{N_{dark} - N_2}{N_{max} - N_{dark}} + 1\right) + \arccos\left(2 \frac{N_{dark} - N_4}{N_{max} - N_{dark}} + 1\right) - \arccos\left(2 \frac{N_{dark} - N_3}{N_{max} - N_{dark}} + 1\right) \right)$$

(see Appendix 1 for derivation of this equation).

When  $\Delta\varphi$  is known, we add it to  $\varphi_0$ , which was measured on the first stage. Then, knowing Bob's modulator half-wave voltage, we simply calculate the appropriate voltage, which we then apply to Bob's phase modulator as the bias voltage for subsequent key transmission cycle, which have to be performed immediately to avoid errors because of phase drift.

To get phase accuracy of, for example,  $15^\circ$ , we will need about 120 detector counts (see Appendix 2). In real QKD situation, when we transmit  $1.3 \mu\text{m}$  photons over 20-km optical fiber and APD detection efficiency is 10%, the estimated count probability will be  $5 \cdot 10^{-4}$  per bit slot. So, to acquire 120 counts, we will need 240000 bits buffer memory. The buffer memory amount in Box 3 is 4 Mbits, so it is enough to satisfy the requirements.

### 7.3. Obtained results

The entire system is controlled by a program mostly written in LabVIEW, with some C code in time-critical routines. The  $\Delta\varphi$ , phase modulator voltage and other values are calculated by this program, and the results are displayed.

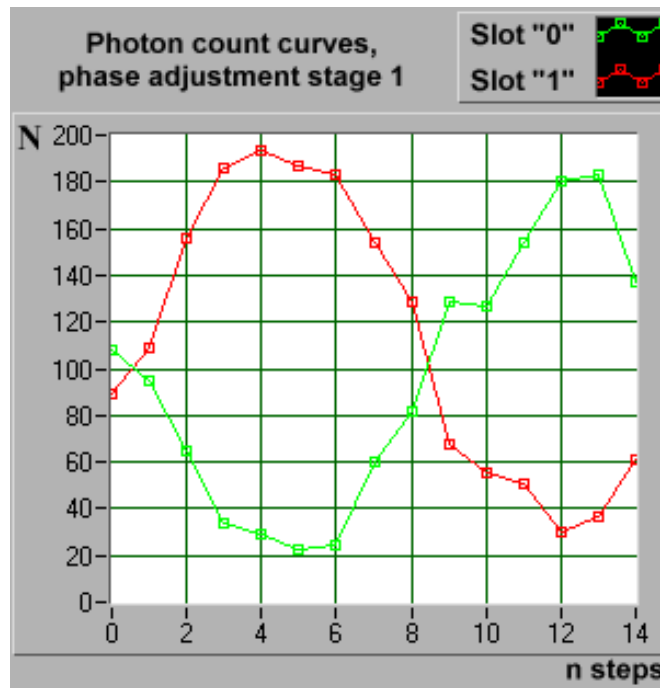


Fig. 11. Phase adjustment stage 1: the number of counts on each step of Bob's PM voltage (15 steps total).

Figure 11 represents measurements taken on the first stage of phase adjustment routine. The curves consist of the numbers of counts in both "0" and "1" time slots for each of 15 steps of voltage, applied to Bob's phase modulator on stage 1. The curves look "noisy" because of a low number of counts acquired on each step. However, the step with minimum number of counts can be easily recognized – this is all we need on this stage. The algorithm actually works reliable with several times fewer counts and much uglier curves than shown here.

The charts of the resulting bias voltage for Bob's phase modulator is shown on figure 12.

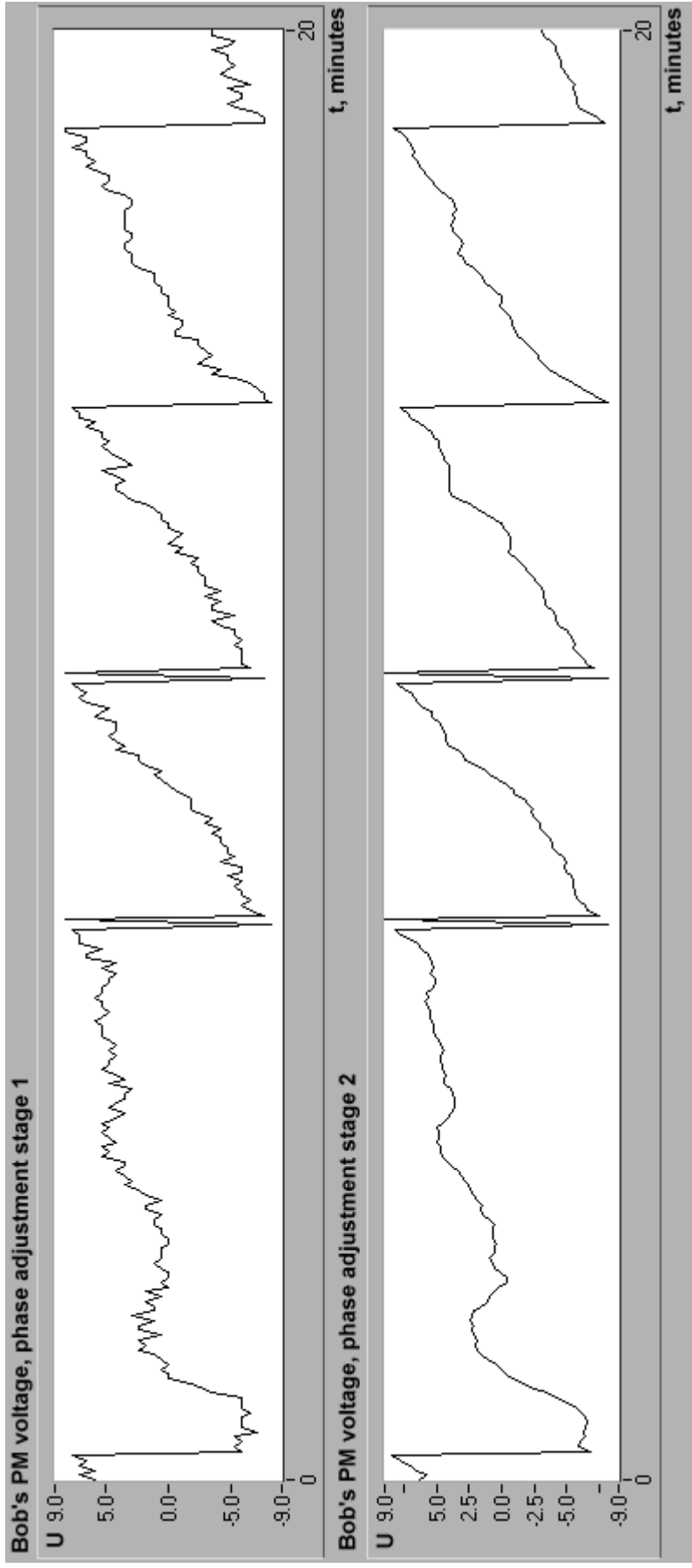


Fig. 12. Resulting bias voltage charts. The top chart shows the results of stage 1, the bottom one shows more precise results of stage 2.

Each iteration (300 iterations total) was taking about 4 seconds. It is mostly due to LabView inefficiency. A program fully written on, for example, C with data acquisition insert written on assembler, would be about 10 times faster. We can increase the performance even more if we perform the intermediate data calculations in hardware right inside of the Box 3. Now, all contents of Box 3's buffer memory (512 KB) is read byte-by-byte, which require 524288 input/output cycles total. In real setup, when the transmission line length is 20 km and detector efficiency is 10%, the count probability is about  $5 \cdot 10^{-4}$ . So, if Box 3 was able to "filter" the incoming information and keep only the cases when detector count had taken place, we would decrease the required number of in/out cycles approximately by the factor of 2000.

As we can see, the phase drifts slowly at the rate not exceeding  $360^\circ$  per several minutes. The speed of this drift changes randomly; sometimes the phase begins to drift in an opposite direction. The "noisy" look of the top chart can be explained by errors due to limited number of steps and limited number of counts acquired on each step in stage 1. The bottom chart looks much smoother, because the  $\Delta\phi$ , calculated on the second stage, compensates for these errors.

The residual noise in the second chart may well be the actual high-frequency component of the phase drift.

#### **7.4. Discussion of results**

Other scientific groups working with phase coding based QKD setups had different approaches to compensate for the phase drift in their interferometers. Wolfgang Tittel and his co-workers [23] are using active thermostabilization of their setup. The interferometers are placed in copper tubes (their lengths are about 40 cm and diameters are 2 cm) filled with sand, thermal sensors are placed inside. Heating wires are reeled on the tubes. The tubes are placed into

thermally isolated containers, and its temperature is stabilized on  $30^{\circ}$  C. In the experiment they slowly (in several hours) increased the temperature of one of the interferometers on  $0.5^{\circ}$  C, and the phase change was 4 full periods [23]. They've made the decision not to implement any active phase adjustment techniques, since after performing the temperature stabilization they haven't noticed any phase drift.

The idea of active thermostabilization is very simple and obvious, but it has its disadvantages. The main disadvantage is its inertness (it takes about several hours to adjust the phase). So, despite the system is thermally stabilized, any mechanical impact on the setup will result in a long period of system's inactivity (while the phase will be adjusting by the means of adjusting the temperature). On the other hand, our setup provides fast phase adjustment (about several seconds are required to adjust the phase), so it can quickly work out any thermal or mechanical impacts.

We have to mention that our setup would not be able to function if the temperature changes in the interferometer were relatively fast, so we use thermal isolation of Alice's and Bob's optical setups. However, the use of any active thermostabilization is not required.

Paul D. Townsend working in BT labs in UK used a piezoelectric transducer to adjust the length of one of the arms of Alice's interferometer [5]. The phase adjustment procedure is performed as follows: Alice and Bob turn their modulators off, and Alice sets her electrically switched attenuator to low to increase the number of photons per pulse. Alice then uses a piezoelectric transducer to adjust rapidly the length of one of the arms in her half of the interferometer, while Bob monitors the count rates from his 0 and 1 output ports. When Bob's 1 count rate is minimized, he sends a trigger pulse to Alice to initiate key transmission. Alice then switches her attenuator to high attenuation to enter the single-photon mode and then begins the key transmission.

The phase drift rate detected by Townsend was 0.6 rad/s [5]. In our setup the phase drift rate is variable, but usually it do not exceed 1 rad/s.

As we see, Townsend's technique requires two additional components - piezoelectric transducer and electrically switched attenuator. Our technique do not requires any of these components – it is able to perform phase adjustment fully in software, which simplifies the whole system, reducing the system costs and increasing reliability.

Now Townsend and his colleagues are testing the new QKD setup [24]. It is based on integrated fiber optic technology, so the optical setups are very small and it is possible to stabilize its temperatures by the means of Peltier elements. The situation is almost the same as in [23] (no other phase drift compensation techniques are implemented), but this time the setup is not so inertness.

## Conclusion

The main goals of this diploma work was to complete and tune the QKD setup and to develop and implement the automatic phase adjustment technique. The phase adjustment, together with passive thermostabilization, is required for the system to function properly when transmitting the key. The use of implemented phase adjustment algorithm can function on a quantum level, which means we are not required to increase the intensity of light propagating in the system while adjusting the phase. It makes possible not to add any other optical components such as variable attenuator, so the system becomes simpler, less expensive and more reliable. The proper functioning of the phase adjustment algorithm testifies that both optical and electronical parts of the setup are tuned and functioning properly. The phase adjustment technique presented here is more advanced than other scientific groups' achievements. There was no key transmission experiment, because the key transmission software is currently under development and will be completed in 2002.

## **Acknowledgements**

I'd like to state my acknowledgements to all people I worked with, in particular to the leader of the project Dag Roar Hjelme for guidance, Vadim Makarov for his invaluable help with hardware, and Astrid Dyrseth for LabView programming.

This research and my stay in Trondheim were financed by the Norwegian Research Council (NFR) under project nr. 119376/431.



## Appendix 1

Calculation of phase correction coefficient for Phase Adjustment stage 2:

$$N_1 = (N_{\max} - N_{\text{dark}}) \sin\left(\frac{\Delta\varphi + 90^\circ}{360^\circ} \pi\right) + N_{\text{dark}}$$

$$N_2 = (N_{\max} - N_{\text{dark}}) \sin\left(\frac{\Delta\varphi - 90^\circ}{360^\circ} \pi\right) + N_{\text{dark}}$$

Determining  $\Delta\varphi$ :

$$\sin^2\left(\frac{\Delta\varphi_a + 90^\circ}{360^\circ} \pi\right) = \frac{N_1 - N_{\text{dark}}}{N_{\max} - N_{\text{dark}}}$$

$$1 - \cos\left(\frac{\Delta\varphi_a + 90^\circ}{180^\circ} \pi\right) = 2 \frac{N_1 - N_{\text{dark}}}{N_{\max} - N_{\text{dark}}}$$

$$\frac{\Delta\varphi_a + 90^\circ}{180^\circ} \pi = \arccos\left(2 \frac{N_1 - N_{\text{dark}}}{N_{\max} - N_{\text{dark}}} + 1\right)$$

$$\Delta\varphi_a = \frac{180^\circ}{\pi} \arccos\left(2 \frac{N_{\text{dark}} - N_1}{N_{\max} - N_{\text{dark}}} + 1\right) - 90^\circ$$

The same calculations using  $N_2$  give us the second approximate value of  $\Delta\varphi$ :

$$\Delta\varphi_b = \frac{180^\circ}{\pi} \arccos\left(2 \frac{N_{\text{dark}} - N_2}{N_{\max} - N_{\text{dark}}} + 1\right) + 90^\circ$$

The final value of  $\Delta\varphi$  can be calculated by averaging  $\Delta\varphi_a$  and  $\Delta\varphi_b$ :

$$\Delta\varphi = \frac{\Delta\varphi_a + \Delta\varphi_b}{2}$$

$$\Delta\varphi = \frac{90^\circ}{\pi} \left( \arccos\left(2 \frac{N_{\text{dark}} - N_1}{N_{\max} - N_{\text{dark}}} + 1\right) - \arccos\left(2 \frac{N_{\text{dark}} - N_2}{N_{\max} - N_{\text{dark}}} + 1\right) \right)$$

As far as we have two bit slots, we will get another results for another bit slot:

$$\Delta\varphi = \frac{90^\circ}{\pi} \left( \arccos\left(2 \frac{N_{\text{dark}} - N_4}{N_{\max} - N_{\text{dark}}} + 1\right) - \arccos\left(2 \frac{N_{\text{dark}} - N_3}{N_{\max} - N_{\text{dark}}} + 1\right) \right)$$

So, the final value of  $\Delta\varphi$  will be:

$$\Delta\varphi = \frac{45^\circ}{\pi} \left( \arccos\left(2 \frac{N_{\text{dark}} - N_1}{N_{\max} - N_{\text{dark}}} + 1\right) - \arccos\left(2 \frac{N_{\text{dark}} - N_2}{N_{\max} - N_{\text{dark}}} + 1\right) + \right. \\ \left. + \arccos\left(2 \frac{N_{\text{dark}} - N_4}{N_{\max} - N_{\text{dark}}} + 1\right) - \arccos\left(2 \frac{N_{\text{dark}} - N_3}{N_{\max} - N_{\text{dark}}} + 1\right) \right)$$

## Appendix 2

Estimating the number of counts to acquire to get 5% phase accuracy

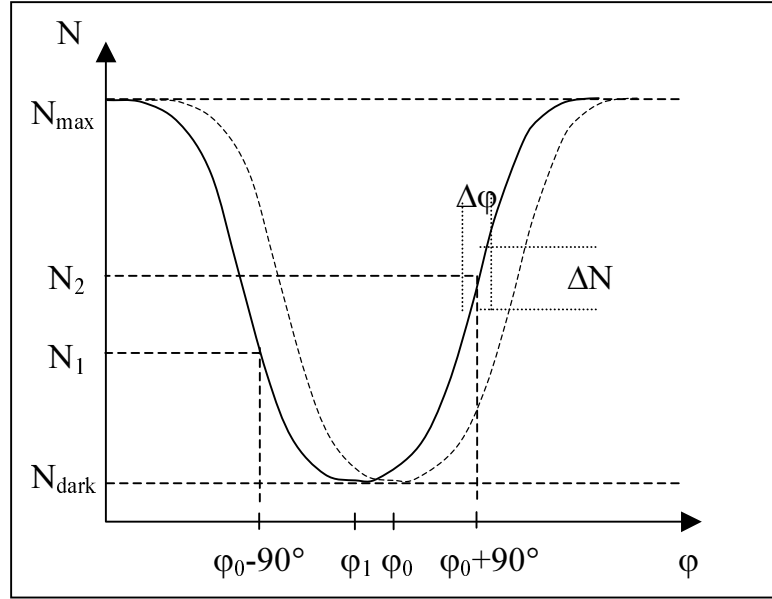


Fig. 13

As we know,  $N = (N_{\text{max}} - N_{\text{dark}}) \sin^2\left(\frac{\phi}{360^\circ} \pi\right) + N_{\text{dark}}$

$$\begin{aligned} \frac{dN}{d\phi} &= (N_{\text{max}} - N_{\text{dark}}) \left( \sin^2\left(\frac{\phi}{360^\circ} \pi\right) \right)' = (N_{\text{max}} - N_{\text{dark}}) \left( \frac{1 - \cos\left(\frac{\phi}{180^\circ} \pi\right)}{2} \right)' = \\ &= \frac{(N_{\text{max}} - N_{\text{dark}})}{2} \left( -\cos\left(\frac{\phi}{180^\circ} \pi\right) \right)' \\ \left. \frac{dN}{d\phi} \right|_{\phi=90^\circ} &= \frac{(N_{\text{max}} - N_{\text{dark}})}{2} \frac{\pi}{180^\circ} \sin \frac{\pi}{2} = (N_{\text{max}} - N_{\text{dark}}) \frac{\pi}{360^\circ} \end{aligned}$$

So,  $\frac{\Delta N}{\Delta \phi} = (N_{\text{max}} - N_{\text{dark}}) \frac{\pi}{360^\circ}$  (see fig. 13).

Now, let  $N_{\text{dark}}=0$ , and let  $\Delta N = 2\sigma = 2\sqrt{\frac{N_{\text{max}}}{2}} = \sqrt{2N_{\text{max}}}$

$$\frac{\sqrt{2N_{\text{max}}}}{\Delta \phi} = N_{\text{max}} \frac{\pi}{360^\circ}; \quad \sqrt{2N_{\text{max}}} = \Delta \phi \cdot N_{\text{max}} \frac{\pi}{360^\circ} \Rightarrow$$

$$\Rightarrow \sqrt{\frac{N_{\max}}{2}} = \frac{360^\circ}{\pi \Delta \varphi}$$

So,  $N_{\max} = \frac{259200}{\pi^2 \Delta \varphi^2} = \frac{26263}{\Delta \varphi^2} \Big|_{\Delta \varphi = 15^\circ} = 117$ . It's the number of counts needed to achieve  $15^\circ$  phase error.

## References

- [1] Simon Singh. The Code Book. Fourth Estate, London, 1999.
- [2] Nicolas Gisin, Gregoire Ribordy, Wolfgang Tittel, Hugo Zbinden. Quantum Cryptography, submitted to *Reviews of Modern Physics*, January 19, 2001.
- [3] Charles H. Bennett et al. Experimental Quantum Cryptography, *Journal of Cryptology*, no. 5, 1992.
- [4] Charles H. Bennett, Gilles Brassard, Artur K. Ekert. Quantum Cryptography, *Scientific American*, October 1992.
- [5] Christophe Marand, Paul D. Townsend. Quantum key distribution over distances as long as 30 km, *Optic Letters*, Vol. 20, No. 16, 1995.
- [6] R. J. Hughes, G. G. Luther, G. L. Morgan, C. G. Peterson and C. Simmons. Quantum Cryptography over Underground Optical Fibers, *Lecture Notes in Computer Science* 1109, 1996.
- [7] R. J. Hughes, G. L. Morgan, C. G. Peterson. Practical quantum key distribution over a 48-km optical fiber network, *Journal of Modern Optics*, 47, 2000.
- [8] Wolfgang Tittel, Gregoire Ribordy and Nicolas Gisin. Quantum Cryptography, *Physics World*, March 1998.
- [9] A. Muller, J. Breguet and N. Gisin. Experimental demonstration of quantum cryptography using polarized photons in optical fiber over more than 1 km. *Europhysics Letters*, 23, 1993.
- [10] A. Muller, H. Zbinden and N. Gisin. Underwater quantum coding, *Nature* 378, 1995
- [11] A. Muller, H. Zbinden and N. Gisin. Quantum cryptography over 23 km in installed under-lake telecom fibre, *Europhysics Letters*, 33, 1996.
- [12] J. D. Franson and B.C. Jacobs. Operational system for Quantum cryptography, *Elect. Letters*, 31, 1995.
- [13] Paul D. Townsend. Secure key distribution system based on Quantum cryptography, *Elect. Letters*, 30, 1994.
- [14] Paul D. Townsend. Quantum Cryptography in Optical Fiber Networks, *Optical Fiber Technology*, 4, 1998.
- [15] Paul D. Townsend. Simultaneous Quantum cryptographic key distribution and conventional data transmission over installed fibre using WDM, *Elect. Letters*, 33, 1997.
- [16] Bennett, C. H., and Brassard, G., Quantum cryptography: Public key distribution and coin tossing. 1984, *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, pp. 175-179.
- [17] Wiesner, S., Conjugate coding, manuscript written circa 1970, unpublished until it appeared in Sigact news, Vol. 15, no. 1, 1983, pp. 78-88.
- [18] See, for example, Okoshi, T., Polarization-State Control Schemes for Heterodyne or Homodyne Optical Fiber Communications. *Journal of Lightwave Technology*, Vol. LT-3, no. 6, 1985, pp. 1232-1237.

- [19] Townsend, P. D., Rarity, J. G., and Tapster, P. R., Single photon interference in 10 km long optical fibre interferometer. *Electronics Letters*, Vol. 29, no. 7, 1993, pp. 634-635.
- [20] Vakhitov, A., Makarov, V., and Hjelme, D. R., Large pulse attack as a method of conventional optical eavesdropping in quantum cryptography. *Journal of Modern Optics*, 2001, Vol. 48, no. 13, pp. 2023-2038
- [21] Martinelli M., A universal compensator for polarization changes induced by birefringence on a retracting beam. *Opt. Commun.*, 1989, vol. 72, pp. 341-344
- [22] Shor, P. W., Algorithms for quantum computation: discrete logarithms and factoring. *Proceedings of the 35<sup>th</sup> Symposium on Foundations of Computer Science*, Los Alamitos, edited by Shafi Goldwasser (IEEE Computer Society Press), 1994, pp. 124-134
- [23] W. Tittel, J. Brendel, H. Zbinden, and N. Gisin. Quantum cryptography using entangled photons in energy-time Bell states. *Phys. Rev. Lett.* Vol. 84, Number 20 (2000).
- [24] EQUIS Project. WP4 - Integrated Mach-Zehnder / Michelson interferometer (P. Townsend and G. Bonfrate from Corning Research, and four more persons from Heriot-Watt University).  
<http://www.phy.hw.ac.uk/resrev/EQUIS/>