PRACTICAL ASPECTS OF QUANTUM CRYPTOGRAPHY

Miloslav Dušek,[1] Ondřej Haderka,[2,1] and Martin Hendrych[2,1]

[1]Department of Optics, Palacký University
[2]Joint Laboratory of Optics of Palacký Univ.
& Phys. Inst. Czech Acad. Sci.
17. listopadu 50, 772 00 Olomouc, Czech Republic

Abstract

An apparatus for quantum key distribution using two unbalanced fibre Mach-Zehnder interferometers has been constructed in our laboratory. Physical aspects qualifying good performance of the system were thoroughly studied. The research covered a matter of coherence properties of the light source, a question of losses, noise, polarization, optimization of detection, problems associated with the decrease of visibility caused by imperfections of beam-splitters and unbalanced losses in different arms of interferometers, and active stabilization of interference (the problem of thermal stability). A quantum identification system has been proposed and tested. It combines a simple classical identification procedure and quantum key distribution, where the latter functions to replace used identification sequencies by new ones. Each identification sequence is used only once. The questions of authentication of public discussion have also been studied.

INTRODUCTION

In everyday life there are many situations when it is necessary to conceal the contents of confidential information conveyed over insecure communications lines. Classical cryptographic techniques have proved very helpful for this task. However, nearly all these techniques are merely computationally secure, i.e., they rely on limited advancement of computer power, technologies, and mathematical algorithms in the foreseeable future. The construction of a quantum computer can seriously menace their security.

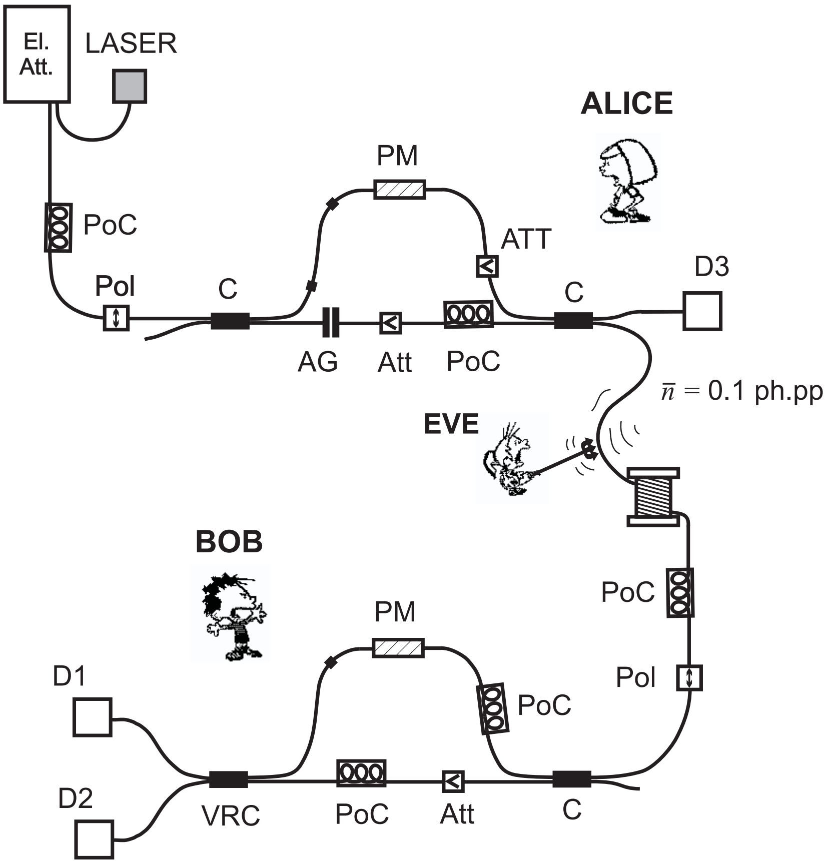

Figure 1. A scheme of optical part of the apparatus. El. Att. – electronic attenuator, PoC – polarization controllers, PM – planar electro-optic phase modulators, Att – attenuators, Pol – polarizers, C – fibre couplers, VRC – variable ratio coupler, AG – air gap.

In the recent past, there has been a good deal of research of a new cryptographic method whose security is based on the fundamental laws of quantum physics – quantum cryptography.[1, 2, 3, 4, 5, 6, 7] Its main triumph is that it can solve the problem of key distribution. From the practical point of view, it is interesting that quantum cryptography may expediently be realized by means of quantum optics. The alphabet is represented by quantum states of electromagnetic field and optical fibre serves as a transmission channel. To encode information, e.g., polarization or phase can be used. The method based on "one-photon" interferometry has been analyzed by our group.

One of the basic cryptographic tasks is to certify the identities of the legitimate users of a communications line. Existing identification systems are only computationally secure. A quantum identification system was first proposed by C. Crépeau and L. Salvail.[8] Their identification protocol is based on quantum oblivious transfer. Alice and Bob mutually check their knowledge of a common secret string without disclosing it. However, quantum oblivious transfer has been proved insecure against the so-called collective attacks by D. Mayers,[9, 10] and H.K. Lo and H.F. Chau.[11] Although to perform collective attacks is not possible with current technology, recent developments suggest that it might be possible in the near future. We propose an identification protocol combining expediently a simple classical identification method with quantum key distribution.[12]

EXPERIMENTAL REALIZATION

Outlines of experimental implementation of our system are given in Fig.1. The apparatus is based on an interferometric setup with time multiplexing. It consists of two unbalanced fibre Mach-Zehnder interferometers. The path difference (2 m) of the arms of each interferometer is larger than the width of the laser pulse (its duration is 4 ns). Interference occurs at the outputs of the second interferometer for pulses "going through" long-short or short-long paths. These paths are of the same length and they are indistinguishable. Each of these interferometers represents the main part of the "terminals" of both communicating parties (called conventionally Alice and Bob). The terminals are interconnected by a 0.5 km single mode optical fibre acting as a quantum channel and also by a classical channel (local computer network). As a light source, a semiconductor laser operating at 830 nm is used. Laser pulses are attenuated by a computer-controlled attenuator so that the intensity level at the output of the first interferometer is 0.1 photon per pulse. The accuracy of this setting is monitored by detector D3. Polarization properties of light in the interferometers are controlled by polarization controllers PoC. To balance the lengths of the arms, an air gap AG with remotely controlled gap-distance is used. The phase coding is performed by means of two planar electro-optic phase modulators PM (one at each terminal). As the last beam splitter a variable ratio coupler VRC is used. With this setup, it is possible to reach visibilities well above 99.6 %. Detectors D1–D3 are single photon counting modules with Si-avalanche photodiodes. Their output signals are processed by detection electronics based on time-to-amplitude converters and single channel analyzers. Both terminals are fully driven by computers. The interferometers are placed in thermo-isolating boxes. Together with automatic active stabilization of interference, it enables us to reach low error rates below 0.4 % with raw data transmission rates of the order of kilobits per second.

WHAT AFFECTS GOOD PERFORMANCE OF THE APPARATUS

An analysis of various physical influences is important for minimizing the device's error – a necessary condition for effective detection of eavesdropping.

Coherence properties of laser pulses used. The coherence length and the shape of the autocorrelation function determine the precision with which it is necessary to balance the lengths of the arms of the interferometer in order to obtain high visibility of interference. In our particular case, to reach visibilities above 99.5 % the path difference of the arms must not exceed 5 μm.

Unbalanced losses and beam-splitting ratios. Fringe visibility in a Mach-Zehnder interferometer is adversely affected by beam-splitter imperfections and unequal losses in its arms. The effect of these factors may be eliminated by inserting additional losses in one of the arms of the interferometer[13]. However, if unity visibilities are required at both detectors, then the last beam splitter must have an ideal 50:50 splitting ratio. This is the reason why we employ a variable ratio coupler as the output beam splitter in our interferometer. (Real beam splitters are "nonunitary", thus the ratio 50:50 is meant between two inputs of the coupler to each output separately.) The additional losses mentioned should be concentrated in Alice's part of the interferometer since losses in Bob's part decrease transmission rates. In our apparatus the losses of Bob's part are about 4.5 dB.

Polarization of light. Fringe visibility further depends on the degree of polarization of light entering the interferometer and, of course, on congruence of polarization states of the beams combined at the output of the interferometer[14]. In our system the degree of polarization of laser radiation is improved by planar phase modulators (placed in both arms) which also serve as polarizers with extinction coefficient 10^{-6}. The changes of polarization states in optical fibres (due to birefringence caused by bending the fibres, etc.) must be compensated for by polarization controllers. Another problem arises because of distortions of polarization on the fibre connecting Alice's and Bob's parts of the interferometer. A partial solution is to place a polarizer in front of Bob's apparatus – then the polarization changes affect the data rate but do not very effect the error rate.

Thermal fluctuations of phase. Fluctuations of temperature and temperature gradients cause changes of refraction indices of fibers. This is the reason for substantial instability of the interference pattern. Both parts of the interferometer must be thermally isolated (we use polystyrene boxes). The environmental perturbations may further be reduced by means of active stabilization of the interferometer. After certain time intervals (during key distribution), constructive interference at one detector and destructive at the other one is found by scanning the phase difference, and "relative zero" is set on the phase modulators. The combination of the passive and active methods of stabilization gives very good results. In our measurements, the period after which the interferometer was calibrated was usually 3 s (the phase deviations were then smaller than $\pi/100$).

Time multiplexing and synchronization. If only one interconnecting fibre is to be used, time multiplexing is necessary. There are three time-separated peaks, but only the middle one "interferes". The separation of the peaks should be as small as possible since small path difference of the arms of the "sub-interferometers" is advantageous (especially due to lower sensitivity to environmental influences). However, the peaks must not overlap – it would decrease visibility. We use separation 10 ns.

Noise of detectors. The dark counts of detectors represent – together with losses on transmission line – the crucial factor limiting the range of quantum cryptographic transmission. We have used detectors based on Si avalanche photodiodes with less then 60 dark counts per sec.

QUANTUM IDENTIFICATION SYSTEM

In this section we briefly describe two protocols for mutual identification that were implemented in our laboratory quantum cryptographic system. In both these protocols, Alice and Bob check their common secret (random) string in a classical way. To prevent from a later misuse, each identification sequence is used only once and the distribution of a new common secret string is achieved by means of quantum key distribution (QKD) based on the BB84 protocol.[1] QKD has recently been proved secure against any collective attack allowed by quantum mechanics,[15, 16] and thus it offers unconditional protection even against eavesdroppers possessing unlimited computational and technological power.

Protocol I (unjammable open channel)

The protocol consists of a three-pass exchange of identification sequences (ISs) and it can be realized as follows (Alice and Bob already share several secret triads of IS):

- Alice and Bob say each other their ordinal numbers of the first unused IS triads in the stack and choose the higher one if they differ.

- - Alice sends the first IS of the triad to Bob.
  - Bob checks whether it agrees with his copy. If not, Bob aborts communication and shifts his pointer to the next triad. Otherwise he sends the second IS of the triad to Alice.
  - Alice compares whether her and Bob's second ISs agree. If not, she aborts communication and shifts her pointer. Otherwise she sends the third IS to Bob. If Bob finds it correct, the identification is successfully finished.
- To replace the used ISs, Alice and Bob "refuel" new ISs by means of QKD and set the pointers to their initial positions.

The three passes are necessary for the following reason: An eavesdropper (Eve) can pretend to be Bob and get the first IS from Alice. Of course, Alice recognizes that Eve is not Bob because Eve cannot send the correct second IS. So Alice aborts connection and discards this triad (i.e., shifts her pointer to the next one). However, later on Eve could turn to Bob and impersonate Alice. She knows the first IS! Bob can recognize a dishonest Eve just only because she does not know the third IS.

Let us note that Alice and Bob can tolerate a certain small number of errors in compared ISs (such that corresponding information leaked to Eve during QKD would not be sufficient for her to succeed in the identification procedure). Thus there is no need to perform error correction and privacy amplification after QKD.

Protocol II (with authenticated public discussion)

In reality, it is difficult to create a physically unjammable communication channel. Therefore unconditionally secure authentication of the messages sent over the open channel is necessary. The authentication of public discussion performed during QKD can be, however, utilized for the identification itself. Three-pass authenticated public discussion can function as the three-pass exchange of ISs described in the Protocol I. Note, that the authentication would anyway require additional "key" material to be prestored and transmitted similarly to ISs. The concrete authentication algorithm employed is based on the so-called orthogonal arrays[17] and is briefly described elsewhere.[12] A more detailed description of the protocol will be given in a separate paper.

- Alice and Bob first perform transmission over the quantum channel according to the BB84 protocol.
- Alice and Bob say each other their addresses in the pool of shared secret information and choose the higher one if they differ. Then a three-pass authenticated public discussion follows:
  - Bob sends to Alice an authenticated message containing the positions of bits randomly selected for error rate estimation.
  - Alice checks authentication and aborts communication if it fails. Otherwise she sends back to Bob an authenticated message containing the bases and bit values of the selected bits.
  - Bob checks authentication and aborts communication if it fails. Next he compares bases of the selected subset and retains only those qubits where his and Alice's bases coincide. At last, he estimates error rate and aborts communication when his result exceeds a certain limit value.[12] If all these three tests are correctly passed, he sends to Alice an authenticated message

to inform her that identification was successful. Alice checks authentication and aborts communication if it fails.

- Alice and Bob compare bases of the rest of their raw data and arrive at their sifted keys.
- Then they perform error correction and privacy amplification procedures and arrive at an error-free distilled key.
- Alice and Bob refuel their shared secret information.

The used authentication sequences are always thrown away. The length of the raw quantum transmission must be selected such that the length of the newly obtained distilled key is greater than the number of bits consumed for authentication/identification purposes. It is convenient if it covers several unsuccessful identification procedures.

It is worth mentioning that the extent of authenticated information transmitted during QKD is limited due to the fact that the authentication procedure consumes a considerable part of the distributed key for its next run. In fact, only a fraction of public discussion can be authenticated. As the crucial characteristic of quantum cryptography is that any attempt at eavesdropping inevitably increases the number of errors in the transmitted key, it is necessary to authenticate just the part of public discussion serving error-rate estimation.[12]

Acknowledgement. The authors wish to express their gratitude to Professor Jan Peřina for his help throughout and for encouragement. This research was supported by Czech Ministry of Education (VS 96028), Czech Grant Agency (202/95/0002) and Czech Home Department (19951997007, 19982003012).

REFERENCES

1. C.H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India* (IEEE, New York, 1984), p. 175.
2. C.H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, J. Cryptology **5**, 3 (1992).
3. A.K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
4. C.H. Bennett, G. Brassard, and N.D. Mermin, Phys. Rev. Lett. **68**, 557 (1992).
5. C.H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).
6. A.K. Ekert, J.G. Rarity, P.R. Tapster, and G.M. Palma, Phys. Rev. Lett. **69**, 1293 (1992).
7. C. Crépeau, in *Proc. 1st Intl. Conf. Theory and Applications of Cryptology, Pragocrypt '96, Prague* (CTU Publishing, Prague, 1996), p. 193.
8. C. Crépeau and L. Salvail, in *Advances in Cryptology: Proc. of Eurocrypt '95,* (Springer-Verlag, 1995), p. 133.
9. D. Mayers, Unconditionally secure quantum bit commitment is impossible, available at http://xxx.lanl.gov/abs/quant-ph/9605044.
10. D. Mayers, The Trouble with Quantum Bit Commitment, available at http://xxx.lanl.gov/abs/quant-ph/9603015.
11. H.-K. Lo and H.F. Chau, Is Quantum Bit Commitment Really Possible?, available at http://xxx.lanl.gov/abs/quant-ph/9603004.
12. M. Dušek, O. Haderka, and M. Hendrych, Acta Physica Slovaca, **48**, 169 (1998).
13. M. Hendrych, M. Dušek, and O. Haderka, Acta Physica Slovaca, **46**, 393 (1996).
14. M. Hendrych, M. Dušek, and O. Haderka, in *Proc. 1st Intl. Conf. Theory and Applications of Cryptology, Pragocrypt '96, Prague* (CTU Publishing, Prague, 1996), p. 234.
15. E. Biham, M. Boyer, G. Brassard, J. van de Graaf, and T. Mor, Security of Quantum Key Distribution Against All Collective Attacks, available at http://xxx.lanl.gov/abs/quant-ph/9801022.
16. D. Mayers and A. Yao, Unconditionally Security in Quantum Cryptography, available at http://xxx.lanl.gov/abs/quant-ph/9802025.
17. D.R. Stinson: *Cryptography, Theory and Practice,* CRC Press, Boca Raton, 1995.