APPLICATION OF QUANTUM KEY DISTRIBUTION FOR MUTUAL IDENTIFICATION – EXPERIMENTAL REALIZATION[1]

M. Dušek[a], **O. Haderka**[ab], **M. Hendrych**[ab]
(*a*) *Department of Optics, Palacký University, 17. listopadu 50,*
772 00 Olomouc, Czech Republic
(*b*) *Joint Laboratory of Optics of Palacký Univ. & Phys. Inst. Czech Acad. Sci.,*
17. listopadu 50, 772 00 Olomouc, Czech Republic

Received 15 May 1998, accepted 24 May 1998

A secure quantum identification system combining a classical identification procedure and quantum key distribution is proposed. Each identification sequence is always used just once and new sequences are “refuelled” from a shared secret key transferred over a quantum channel. The question of authentication of information sent over a public channel is discussed. An apparatus using two unbalanced Mach-Zehnder interferometers has been built, and quantum key distribution and “quantum identification” have been successfully tested through a single-mode optical fibre at 830 nm, employing low intensity coherent states (below 0.1 photons per pulse).

1. Introduction

Along with the rapid increase in the number of electronic communications grows the need for secure identification systems. Nowadays, various identification systems are employed for financial transactions performed over computer networks, for money withdrawal from automated teller machines, for diplomatic and military purposes, and so on. Even the best classical identification systems, however, do not provide sufficient security with respect to recent advances in the field of quantum physics. An eavesdropper listening in on identification acts of the legitimate users might later misuse the overheard information and try to impersonate them.

In this paper, a secure identification system is proposed, that combines a classical three-pass identification procedure and quantum key distribution (QKD). A large number of papers have already been devoted to quantum cryptography. Let us mention only some of the fundamental ones [1-7] and the survey in [8]. A large bibliography may also be found in [9].

[1] Special Issue on Quantum Optics and Quantum Information

In Section 2 we describe the identification protocol. Section 3 deals with the necessary authentication of the public discussions performed during QKD. Section 4 is devoted to the description of the experimental apparatus. In Section 5 practical realization is described and some experimental results are presented. Section 6 gives conclusions.

2. Identification protocol

The proposed identification protocol is based on a simple classical three-pass identification method using each time a new triad of identification sequences (i.e. the sequences are changed after each identification act, either successful or unsuccessful). This method is secure: a sufficient length of identification sequences exists such that the probability of successful deception by an unauthorized user is smaller than an arbitrarily small positive number. The weak side of classical implementations of this method is the problem of delivering of secret identification sequences (IS's). To circumvent this difficulty, the well known quantum key distribution procedure (QKD), based on BB84 protocol [1], is employed. QKD represents the "quantum part" of the protocol. At the beginning some small amount of secret information must be shared by the users. But after mutual identification, the used IS's are replaced by new ones, distributed by means of QKD. A limited number of IS's could be stored, e.g., on a chip card.

A three-pass identification protocol can be realized as follows (two legal users, Alice and Bob, already share several triads of IS's):

- Alice and Bob say each other their ordinal numbers of IS triads in the stack – a pointer to the first Alice's (Bob's) unused sequence – 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 IS's 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 IS's, Alice and Bob "refuel" new IS's 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 the 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.

3. QKD with authenticated public discussion

Necessary discussions performed over the open (classical) channel during QKD *could* on principle be modified by Eve. So their authentication is necessary. The authentication procedure requires some additional "key" material to be stored and transmitted similarly to IS's. Again, each "key" may be used just once. This authentication, however, can be utilized for the identification itself. The three-pass authenticated public discussion, performed during QKD, can function as the three-pass exchange of IS's described in the preceeding section.

For quantum cryptography to provide unconditional security, the procedure used for authentication of public discussion *must* also be unconditionally secure, not only computationally. Such authentication algorithms have been discovered [10]. These algorithms are based on the so-called orthogonal arrays [11]. It can be shown, however, that the length of an "authentication key" must always be greater than the length of the authenticated message. If k is the number of all possible messages, κ the number of keys, and n the number of all possible authentication tags, using methods of orthogonal arrays theory, it can be proved that $\kappa \geq k(n-1)+1$. It is evident that

$$\kappa > k, \text{ if } n \geq 2.$$

This fact represents a difficulty for QKD. The length of messages communicated over the public channel is always greater than the length of the transmitted "quantum" key. For each qubit, at least one bit of information about the basis chosen by Alice, and one bit about the basis chosen by Bob must be interchanged. Only about one half of all successfully conveyed qubits can be used as a key, as follows from the requirement of coincidence of bases. Further, part of the key has to be sacrificed and compared by Alice and Bob in order to detect possible eavesdropping. So there would not be enough "quantum" key material for refueling new authentication keys for next authentications. A way out from this impasse rests in realizing that it is not necessary to authenticate the whole public discussion performed during QKD. The most important and characteristic property of quantum cryptography is that it enables us to detect an eavesdropper. Any attempt at eavesdropping inevitably increases the number of errors. Thus it is necessary to prevent Eve from modifying in any way the part of public discussion connected with the error rate estimation. Therefore, messages containing the sacrificed part of the "quantum" key (including corresponding bases and positions of sacrificed bits) have to be authenticated. Any modification of the rest of public communications could impair QKD but would not jeopardize the security of the system. Nevertheless, there is still a loophole. Eve could establish one "quantum" key with Alice and a different one with Bob, and then choose only those bits that are identical in both keys. Then she could manipulate public discussion in such a way that Alice and Bob would consider the remaining bits to be lost or invalid. To prevent this from happening, Alice and Bob must in addition exchange an authenticated message conveying the number of really detected qubits.

As already mentioned, a class of reasonable authentication codes exists [10]. If p is prime and $d \geq 2$ is an integer, then an authentication code can be created for $(p^d -$

$1)/(p-1)$ messages with p^d keys and p authentication tags. The deception probability is then p^{-1}. For a given message and a given authentication key, the authentication tag can be calculated as follows:

- Convert a given authentication key to the number system of the base p (its maximum length in this system is d). Let us denote the i-th "digit" by r_i.
- Construct and order all non-zero "numbers" in the number system of the base p of the maximum length d that have the first non-zero "digit" from the left equal to 1 [there is $(p^d-1)/(p-1)$ of such numbers]. A one-to-one mapping exists between all possible messages and all "numbers" (or sequences) from this set. Assign a corresponding "number" to a given message to be authenticated (an ordering of the "numbers" is assumed to be fixed). Let the i-th "digit" of that particular "number" be denoted by c_i.
- The authentication tag is then given by the equation

$$A(r,c)=\sum_{i=1}^{d} r_i c_i \bmod p.$$

As a practical example we can choose a prime $p=2^{61}-1$ and $d=165$. Then the deception probability is about $5\cdot 10^{-19}$. The length of the key is 10064 bits, the length of the message can be up to 10003 bits and the authentication tag consist of 61 bits.

4. Description of the apparatus

Experimental implementation of our system is based on an interferometric setup (i.e., on phase coding) with time multiplexing. It consists of two unbalanced fibre Mach-Zehnder interferometers (see Fig. 1). The path difference of the arms of each interferometer (2 m) 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. The terminals are interconnected by a 15 m single mode optical fibre acting as a *quantum channel* and also by a classical channel (local computer network). As a light source, a semiconductor pulsed laser operating at 830 nm is used. Laser pulses are attenuated by a precise computer-controlled attenuator so that the intensity level at the output of the first interferometer is below 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). To achieve high interference visibility, the splitting ratio of the last combiner must approach 50:50 as closely as possible (see [12]). Therefore a variable ratio coupler VRC is employed there. With this setup, it is possible to reach

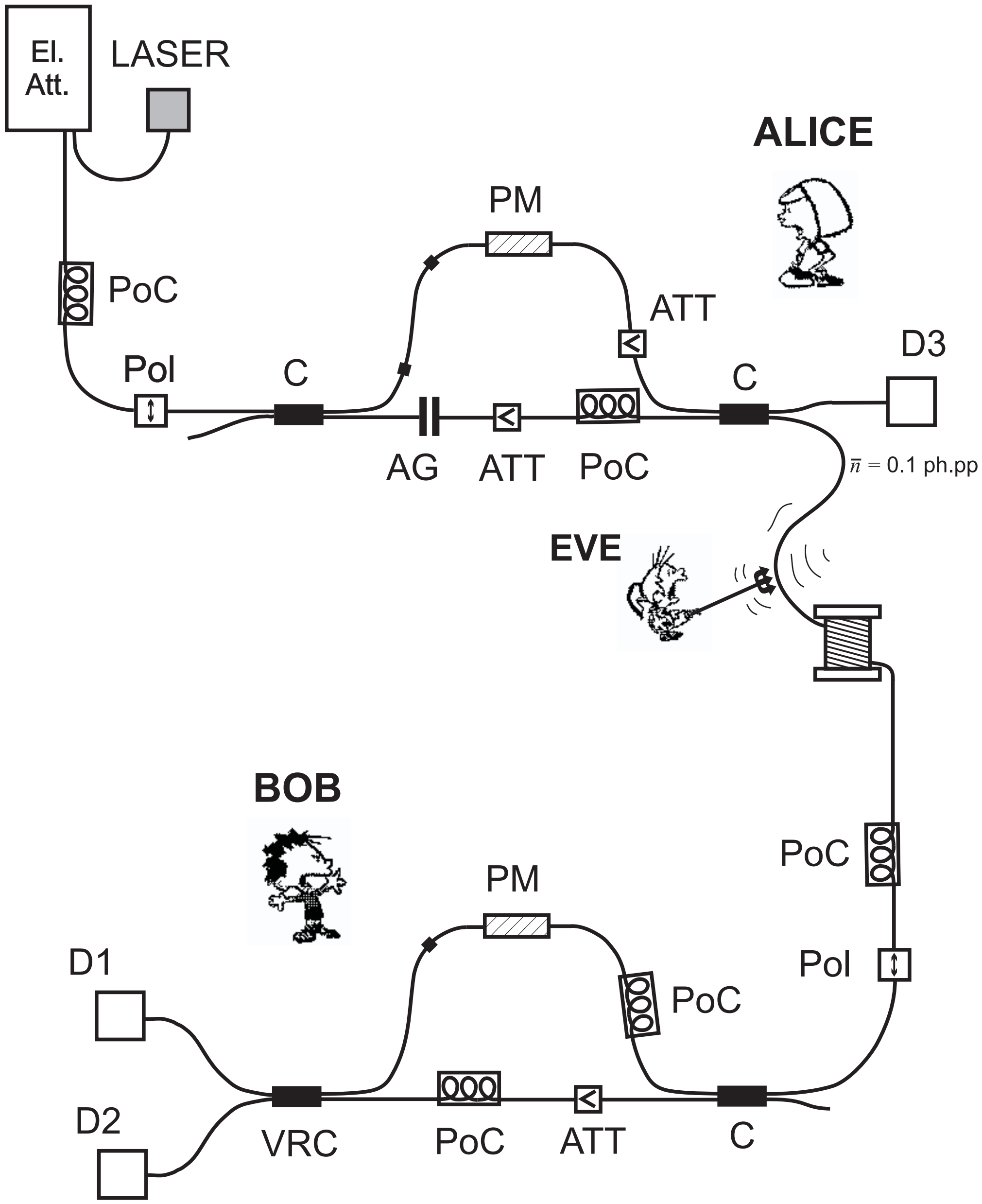

Fig. 1. The scheme of optical part of the built quantum identification system. El. Att. is an electronic attenuator, PoC denotes a polarization controller, PM a planar electro-optic phase modulator, ATT an attenuator, Pol a polarizer, C a fibre coupler, VRC a variable ratio coupler, and AG an air gap.

visibilities well above 99 %. The total losses of the second interferometer do not exceed 5 dB.

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 PC's. The interferometers are placed in polystyrene thermo-isolating boxes. Together with automatic active stabilization of interference, it enables us to reach low error rates (0.4–0.8 %) with data transmission rates of approximately 600 bits per second.

5. Practical implementation

Let us first focus on the part of public discussion that must be authenticated, i.e., on the comparison of Alice's and Bob's subsets of the "random" key, that serves for error rate estimation and thereby the detection of possible eavesdropping. The positions of selected bits must be completely random so that Eve has no hint which bits are "safer" for her to intercept. The length of the subset must be large enough to yield a confident error rate estimate. Let us introduce a *security parameter* q that expresses this confidence in the following way. Provided that the estimate based on a subset of length s is $\varepsilon_{\mathrm{est}}$, the probability that the actual error rate ε of transmission exceeds a certain prescribed limit $\varepsilon_{\mathrm{lim}}$, must be lower then q. The security limit for yet secure QKD is $\varepsilon_{\mathrm{lim}} = 14.6$ % [13]. Once a suitable length s for the system is chosen, one can obtain an upper limit $\varepsilon_{\mathrm{max}}$ on $\varepsilon_{\mathrm{est}}$, above which the transmitted "quantum" key must be rejected to guarantee security with confidence $1-q$. A detailed analysis of the limit on $\varepsilon_{\mathrm{est}}$ is beyond the scope of this paper. For our system, we have chosen $s = 500$ and $q = 10^{-20}$. Then the condition $\mathrm{Prob}(\varepsilon > 0.146) < 10^{-20}$ is satisfied when estimated error rates $\varepsilon_{\mathrm{est}}$ fall below $\varepsilon_{\mathrm{max}} = 2.13$ %.

To authenticate the number of really detected qubits, and the positions, bases and values of qubits from a subset of length s, we need at least

$$b_{\mathrm{min}} = s([\log_2 n] + 2) + [\log_2(\eta n)] + 3a)$$

bits of initially shared secret key material. Here n is the number of sent laser pulses, η is the detection probability (about 0.7 % in our case), $[x]$ denotes the smallest integer larger than x, and $a = [\log_2(1/q)]$ is the length of the authentication tag. It is worth noting that the ratio $b_{\mathrm{min}}/(\eta n)$ converges to zero for large n so that it is always possible to generate more new shared secret bits than it is consumed for authentication. Authenticated QKD may be considered as a "multiplier" of shared secret information, once the ratio $(\gamma\eta n)/(2b_{\mathrm{min}})$ is greater than 1, with γ being the typical reduction factor of the error correction and privacy amplification procedures [2].

The whole identification procedure starts with the generation of the so-called sifted key. Sifted key is what remains to the users after the comparison of their bases. In our experimental setup, we generate sifted key at sequences of 320 kbits. After each sequence, active stabilization of the interferometers is performed to ensure low error rate despite environmental perturbations. This yields an average sifted key data rate of cca 600 bits per second. Once 30 kbits of sifted key are generated, the three-pass authenticated public discussion is performed as follows:

- Bob sends to Alice an authenticated message containing the number of detected qubits and the positions of bits 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 qubits.

- Bob checks authentication and aborts communication if it fails. Next he checks bases of the selected subset and aborts communication if any of them disagree. At last, he uses the comparison of bit values of the selected subset for error rate estimation and aborts communication when his result exceeds the value $\varepsilon_{\max}$. 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.

At this point Alice and Bob share 29.5 kbits of shared secret sifted key. As final steps, they perform error correction and privacy amplification procedures. We basically use the procedures described by Bennett *et al.* [2]. The level of privacy amplification corresponds to the security parameter q.

To summarize, γ is usually higher than 0.75 for our usual error rates of 0.4–0.8 %, thus leaving Alice and Bob with about 22 kbits of distilled key generated at an average rate of 250 bits per second. This well covers the approximately 14 kbits of previously shared secret key material consumed during the authenticated discussion. Let us note that we did not perform any special optimization of data rate, the bottlenecks being here the way we drive the equipment from PC's and the bandwidth of the detection electronics we used. Nevertheless, in our setup the whole identification procedure takes less than 110 seconds (including all auxiliary processes).

6. Conclusions

A quantum cryptographic system for mutual identification has been proposed and built. The system expediently combines the advantages of quantum key distribution and a classical three-pass identification procedure. Each identification sequence is used only once and quantum key distribution serves as a means to refuel shared secret key material. The quantum cryptographic apparatus can be regarded as a "multiplier" of shared secret information. The experimental implementation is based on a "single-photon" interferometric method and on the quantum key distribution protocol BB84. Error correction and privacy amplification procedures are employed. The authentication of certain parts of public discussion simultaneously serves for mutual identification. The measured physical parameters are as follows: visibility 99.5 %, sifted key transmission rate 600 bits per second, distilled key transmission rate 250 bits per second, error rate 0.4 %.

Acknowledgement This work was supported by the Czech Home Department (19951997007), Czech Ministry of Education (VS 96028), and Czech Grant Agency (202/95/0002).

References

[1] C.H. Bennett, 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, J. Smolin: *J. Cryptology* **5** (1992) 3

[3] A.K. Ekert: *Phys. Rev. Lett.* **67** (1991) 661

[4] C.H. Bennett, G. Brassard, N.D. Mermin: *Phys. Rev. Lett.* **68** (1992) 557

[5] C.H. Bennett: *Phys. Rev. Lett.* **68** (992) 3121

[6] A.K. Ekert, J.G. Rarity, P.R. Tapster, G.M. Palma: *Phys. Rev. Lett.* **69** (1992) 1293

[7] C. Crèpeau: in *Proc. 1st Intl. Conf. Theory and Applications of Cryptology, Pragocrypt'96,* Prague, Czech Rep. (CTU Publishing, Prague,1996) p. 193

[8] G. Brassard: in *Proc. 1st Intl. Conf. Theory and Applications of Cryptology, Pragocrypt'96,* Prague, Czech Rep. (CTU Publishing, Prague,1996) p. 183

[9] available at *http://www.IRO.UMontreal.ca/ crepeau/Biblio-QC.html*

[10] D.R. Stinson: *Cryptography, Theory and Practice* (CRC Press, Boca Raton, 1995)

[11] T. Beth, D. Jungnickel, H. Lenz: *Design Theory* (Bib. Institut, Zurich, 1985)

[12] M. Hendrych, M. Dušek, O. Haderka: *acta physica slovaca* **46** (1996) 393

[13] C. Fuchs, N. Gisin, R.B. Griffits, C-S. Niu, A. Peres: *Phys.Rev. A* **56** (1997) 1164