acta physica slovaca vol. 47 No. 3/4, 211 – 216 June 1997

QUANTUM CRYPTOGRAPHY: TOWARDS REALIZATION IN REALISTIC CONDITIONS[1]

N. Imoto[2], M. Koashi, K. Shimizu
NTT Basic Research Laboratories,
3-1 Morinosato-Wakamiya, Atsugi-shi, Kanagawa 243-01, Japan

B. Huttner
Universite de Geneve, GAP-optique,
20, Rue de l'Ecole de Medecine CH1211, Geneve 4, Switzerland

Received 11 May 1997, accepted 12 May 1997

Many of quantum cryptography schemes have been proposed based on some assumptions such as no transmission loss, no measurement error, and an ideal single-photon generator. We have been trying to develop a theory of quantum cryptography considering realistic conditions. As such attempts, we propose quantum cryptography with coherent states, quantum cryptography with two-photon interference, and generalization of two-state cryptography to two-mixed-state cases.

1. Introduction

In these years, our understanding of quantum mechanics is shifting from mere recognition to application of its bizarre properties. The superposition principle and entanglement allow us to perform the parallel processing of an exponentially large number of computing steps (quantum computing) [1]-[3], and the non-cloning theorem [4] prohibits any eavesdropping attempt, which allows us to construct secure means of private key distribution (quantum cryptography) [5]-[10]. Although quantum computing is considered to be difficult to realize, quantum cryptography is already at the stage of experiment [11]. In many of the proposals of the quantum cryptography, however, only ideal situations are assumed, such as no transmission loss, no measurement error and no photon-number uncertainty. These assumptions are never met in true situations, and thus the investigation will be meaningless unless we have a theoretical guarantee for the security of quantum cryptography in non-ideal cases. We have been developing the theory of quantum cryptography considering realistic conditions. As such attempts, we propose quantum cryptography with coherent states [12], quantum cryptography with two-photon interference [13], and generalization of two-state cryptography to two-mixed-state cases [14]. This article is to give an overview of these studies.

[1]Presented at the **Fifth Central-European Workshop on Quantum Optics**, Prague, Czech Republic, April 25 - 28, 1997

[2]E-mail address: nobu@will.brl.ntt.co.jp

2. Quantum cryptography with coherent states

The basic idea of this proposal was motivated by a question: Can the "four-state cryptography [5]" and the "two-state cryptography [7]" be combined in a compatible way to construct a new scheme which is better than any of the two schemes? The answer is "yes" as has been shown in [12]. An ideal single photon source is assumed in the four-state cryptography, whereas coherent states emitted by a usual laser are available in the two-state cryptography. In the newly proposed scheme, the merit of the two-state cryptography is fully used, and the security is also enhanced by the use of the four-state cryptography principle.

In the four-state cryptography, four polarization states of a single photon are used to encode a bit information for private key distribution. Two of them form orthogonal basis and used for encoding "0" and 'M1", and the rest of two form the other orthogonal basis and used in the same way, but any one of the former two states and any one of the latter two states are chosen to be non orthogonal. Whether the sender (Alice, hereafter) uses the former basis or the latter basis is hidden to the receiver (Bob, hereafter) and the eavesdropper (Eve, hereafter). Assuming that Alice sends "0" and "1" with an equal probability, it can be shown that the density operator for Bob (which is also the density operator for Eve) when Alice chooses the former basis is equal to the density operator when Alice chooses the latter basis. Using the non-cloning theorem, it is shown to be impossible for Eve to duplicate such a state. Thus, any attempts of eavesdropping without being detected by Alice and Bob will fail. Of course, Bob does not know Alice's choice, either. However, by choosing the basis independently, and afterwards discarding the photons that are known to be measured with different basis, Alice and Bob can construct their private key with the rest of photons.

In the two-state cryptography, two coherent states having π phase difference containing less than 1 average photons per pulse are used for encoding "0" and "1". Since both of the two coherent states are close to the vacuum, they are far from orthogonal to each other. Therefore, it is not possible for Eve to duplicate the two states again due to the non-cloning theorem. This makes Eve impossible to eavesdrop the bit without being detected by Alice and Bob. Of course, Bob is not able to separate the two states, either. By means of homodyne detection, however, Bob can sometimes detect the photons and tell the phase with certainty. Selecting those pulses which were successfully detected by Bob, Alice and Bob can construct their private key.

In our proposal [12], four coherent states with 0, $\pi/2$, π, and $3\pi/2$ phases containing less than 1 average photons are used. Two of them, 0 and π, are used as (non orthogonal) basis for "0" and "1", and the rest of two, $\pi/2$ and $3\pi/2$, are used in the same way. After Bob's detection, the pulses are selected based on not only whether Bob detected a photon or not but also whether Alice and Bob chose the same basis or not. In this case, Eve may make a mistake in eavesdropping either because she does not know the choice of the basis or because she cannot always separate "0" and "1". This doubled burden to Eve makes our scheme better in performance than any one of the four-state cryptography and the two-state cryptography with coherent states. A quantitative comparison of performance can be made by calculating the mutual information between Alice and Eve or between Eve and Bob normalized to the probability

of detecting Eve. The detailed calculation shows that the leaked information to Eve in our scheme is always less than that of the four-state cryptography and that of the two-state cryptography [12].

3. Quantum cryptography using two-photon interference

In the four-polarization-state cryptography [5] and in those schemes utilizing single-photon interference [7] [10] [12], the optical phase fluctuation in the transmission line significantly affects the detection error at Bob's side. Therefore, Alice and Bob should always calibrate the scheme by compensating the fluctuation to assure that they have the identical definition of polarization or phase. This can be difficult because Alice's phase adjustment, Bob's phase adjustment and transmission line phase noise affect each other.

Cryptography using two-photon interference [8] was proposed to avoid this difficulty. This scheme is an application of the Franson interferometer, in which the coincidence counting of entangled photon pair at the two output ports exhibits $\cos(\theta_A + \theta_B)$ dependence due to the two-photon interference, where θ_A and θ_B respectively are the phase shifts inserted in the Alice's delay line and Bob's delay line. Since this interference effect is nonlocal, the interference is not affected by the phase fluctuation outside the two delay lines. This means that Alice should only concern the fluctuation in her delay line and Bob should only concern the fluctuation in his delay line. Thus, Alice and Bob can adjust their delay lines independently.

In the scheme in [8], however, the coincidence counting is performed between Alice's detector and Bob's detector. This can be practically inconvenient because precise clocks synchronized between the distant two points are needed. To avoid this problem, we have proposed a scheme using two-photon interference in which the coincidence counting is performed only on Bob's side.

Fig. 1 shows the schematic view of a possible configuration for our proposal. Two photons generated by parametric down conversion are sent to the two arms of the scheme. Alice and Bob agrees that they independently choose between coding 1 and 2 randomly. In coding 1, Alice modulates the phase with $\theta_A = 0$ and π for bit "0" and "1", respectively, and Bob sets $\theta_B = 0$. In coding 2, Alice modulates the phase with $\theta_A = \pi/2$ and $3\pi/2$ for bit "0" and "1", respectively, and Bob sets $\theta_B = \pi/2$. The two-photon interference only allows specific pairs of detectors for the coincidence counting at Bob's side due to the $\cos(\theta_A + \theta_B)$ dependence. The possible coincidence counting results are summarized in Table 1 for all combinations of Alice's choice and Bob's choice. One can see that Bob can obtain the bit value only when they choose the same coding. It is also easy to see that Alice's two states corresponding to "0" and "1" are orthogonal within any of coding 1 or 2, but that any state in coding 1 and any state in coding 2 are non orthogonal having $\pi/4$ angle in the Hilbert space. This is exactly the same situation as in the four-polarization-state cryptography. The principle of this scheme is, therefore, nothing but that of the four-polarization-state cryptography. It is obvious, however, that no arbitrary-polarization-maintaining fibre is required and no phase fluctuation compensator is required. Also, Alice and Bob need not have a

common clock because it is only Bob who should watch the coincidence counting.

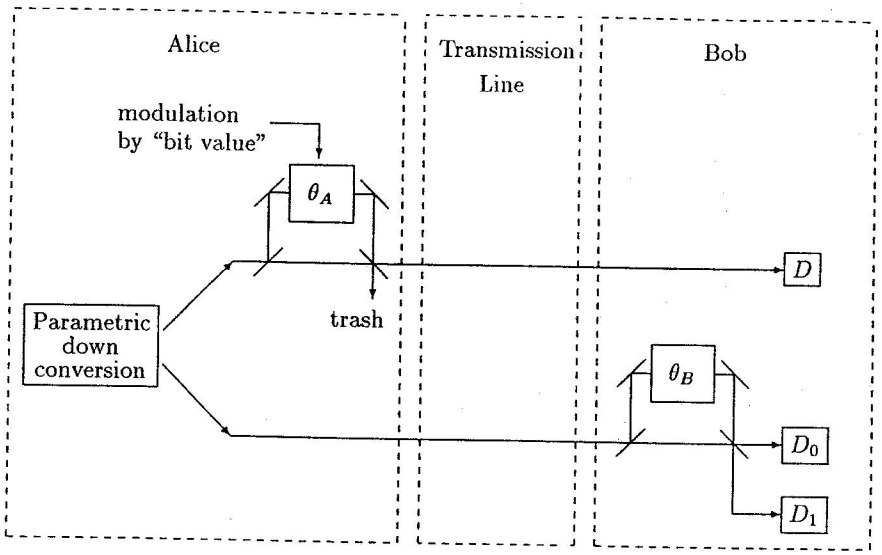

Fig. 1. An implementation of proposed quantum cryptography using two-photon interference. The coincidence counting is performed only at Bob's side.

bit value	0				1			
Alice's choice	Coding 1		Coding 2		Coding 1		Coding 2	
$\rightarrow \theta_A =$	0		$\pi/2$		π		$3\pi/2$	
Bob's choice	Coding 1	Coding 2	Coding 1	Coding 2	Coding 1	Coding 2	Coding 1	Coding 2
$\rightarrow \theta_B =$	0	$\pi/2$	0	$\pi/2$	0	$\pi/2$	0	$\pi/2$
Coincidence counting detector pair	definitely D & D_0 only	D & D_0 or D & D_1	D & D_0 or D & D_1	definitely D & D_1 only	definitely D & D_1 only	D & D_0 or D & D_1	D & D_0 or D & D_1	definitely D & D_0 only

Table 1. Coincidence counting pair for possible combination of the bit value, Alice's choice, and Bob's choice.

4. Quantum cryptography based on two mixed states

In any scheme proposed so far, the states prepared by Alice have been assumed to be pure states. In the real situations, however, the light source usually has excess noise, which requires Alice's states to be expressed by mixed states, and so far, there has been no attempt to treat such cases in the theory of quantum cryptography.

As the first step of such attempt, we have considered the generalization of the Bennett's two-state scheme to mixed state cases [14]. The outline of the theory is as follows: Assuming that the states prepared by Alice are mixed states, Eve can have a variety of options in handling the quantum signal on the way of the transmission line. We consider possible four eavesdropping strategies step by step, and obtain, in each step, a necessary condition to defend the communication from Eve's attack. The necessary condition is therefore becomes severer step by step, and the finally obtained condition is the necessary condition for the security against the four kinds of Eve's attack. This final condition is also shown to be a sufficient condition for the security against *any* kind of Eve's attack. The obtained necessary and sufficient condition thus gives a guiding principle in constructing a two-state cryptography with noisy light sources.

The result of this study gives a simple expression for the necessary and sufficient condition for the security of the two-mixed-state cryptography, which is described as

$$\rho^{(1)} = R(\theta)\rho^{(0)}R^{\dagger}(\theta)\,, \tag{1}$$

where $\rho^{(0)}$ and $\rho^{(1)}$ are the mixed states prepared by Alice, and $R(\theta)$ is a rotation operator defined by a direct product of $R_i(\theta)$ as

$$R(\theta) \equiv \prod_{i=1}^{n} R_i(\theta)\,, \tag{2}$$

where $R_i(\theta)$'s are rotation operator in 2-dimensional Hilbert subspaces properly defined to give a decomposition of the full Hilbert space to make a subspace-conserving projection possible, and n is the dimension of the Hilbert subspace spanned by $\rho^{(0)}$ (which is shown to be the same for the Hilbert subspace spanned by $\rho^{(1)}$) [14]. Eq.(1) tells that the structure of the two mixed states must be identical in the sense that the states are connected by a rotation operator.

4. Discussion

It is important to develop the theory of quantum cryptography considering the reality because all of the studies can become meaningless without knowing the conditions for the security of quantum cryptography in non-ideal cases. Privacy amplification is of course a logical approach for this purpose, but it is "amplification" of security if there is any. It is thus important to examine the security itself under realistic conditions from the fundamental point of view. Not only for this practical reason, we believe that there is a necessity to do so to find a more general, systematic principle, which may be deduced from the case studies of quantum mechanics and information control under different circumstances. As such attempts, we have proposed quantum cryptography with coherent states (attempt to use a normal light source with higher security), quantum cryptography with two-photon interference (attempt to avoid the loss effect and a complex interferometer stabilization), and generalization of two-state cryptography to two-mixed-state cases (attempt to find the security condition with a noisy light source). We hope that these step-by-step considerations will reveal the essence of the quantum information processing.

Acknowledgements We thank to N. Gisin of University of Geneva, T. Mor of the Technion-Israel Institute of Technology, and M. Werner of NTT Basic Research Laboratories for the fruitful discussions and collaborations.

References

[1] D. Deutsch: *Proc. R. Soc. London, Ser. A* **400** (1985) 97

[2] P.W. Shor: in *Proc. 35th Annual Symposium on Foundations of Computer Science* (IEEE Computer Society Press, New York, 1994) p.124

[3] A. Ekert, R. Jozsa: *Rev. Mod. Phys.* **68** (1996) 733

[4] W.K. Wooters, W.H. Zurek: *Nature* **299** (1982) 802

[5] C.H. Bennet, G. Brassard: in *Proc. of IEEE Int. Conf. on Computers, Systems and Signal Processing*, Bangalore, India (IEEE, New York, 1984) p.175

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

[7] C.H. Bennett: *Phys. Rev. Lett.* **68** (1992) 3121

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

[9] C.H. Bennett, S.J. Wiesner: *Phys. Rev. Lett.* **69** (1992) 2881

[10] L. Goldenberg, L. Vaidman: *Phys. Rev. Lett.* **75** (1995) 1239

[11] C.H. Bennett, F. Bessette, G. Brassard, L. Salvail: *J. Cryptol.* **5** (1992) 3; A. Muller, J. Breguet, N. Gisin: *Europhys. Lett.* **23** (1993) 383; J.D. Franson, H. Ilves: *Appl. Opt.* **33** (1994) 2949

[12] B. Huttner, N. Imoto, N. Gisin, T. Mor: *Phys. Rev. A* **51** (1995) 1863

[13] N. Imoto, M. Werner, M. Koashi: in *Technical Digest, XXth International Quantum Electronics Conference IQEC'96* (Sydney, Australia, July 14-19, 1996) p. 271

[14] M. Koashi, N. Imoto: *Phys. Rev. Lett.* **77** (1996) 2137

[15] J.D. Franson: *Phys. Rev. Lett.* **62** (1989) 2205; J.D. Franson: *Phys. Rev. Lett.* **67** (1991) 290