JOURNAL OF MODERN OPTICS, 2003, VOL. 50, NO. 6–7, 1071–1077

Security of the private quantum channel

JAN BOUDA† and VLADIMÍR BUŽEK‡§

† Faculty of Informatics, Masaryk University, Botanická 68a, 602 00 Brno, Czech Republic

‡ Research Center for Quantum Information, Slovak Academy of Sciences, Dúbravská Cesta 9, 842 28 Bratislava, Slovakia; e-mail: buzek@savba.sk

§ Department of Mathematical Physics, National University of Ireland, Maynooth, Ireland

(*Received 10 September 2002*)

Abstract. We extensively discuss the problem of encryption of quantum information. We present an attack on the private quantum channel which applies when partial classical description of the cipher text is known (the known-ciphertext attack) and show how to avoid this situation. The quantum analogue of the known-plaintext attack is also discussed.

1. Introduction

Quantum cryptography is a rapidly developing branch of quantum information processing. The most fundamental results of quantum cryptography include quantum distribution of the key [1, 2], quantum secret sharing [3, 4], quantum oblivious transfer [5] and other cryptographic protocols [6]. Quantum cryptography has two main goals. The first is to ensure the transmission (or manipulation) of *classical* information in the way that the security is guaranteed by laws of quantum mechanics in contrast with classical cryptographic protocols which are based mainly on some arguments from complexity theory. The other goal is to ensure secure manipulation of quantum information, such as secret sharing of quantum information [4].

The rapid development of quantum cryptography has lead to the formulation of the encryption of quantum information defined in terms of the so-called quantum private channel [7], in which the plaintext is quantum information, the transmission channel is quantum while the key is either quantum or classical. As a consequence, we do not have to care about secure distribution of quantum information (as in [3]), but we can concentrate our attention on the protocol itself. A different method of encryption of quantum information which uses entanglement as the key was proposed by Leung [8].

In section 2 we define the private quantum channel as well as the quantum one-time pad. In section 3 we assume an attack against the private quantum channel which applies when Eve obtains at least partial classical information about the ciphertext. We determine the situations when this problem arises and describe how to avoid them. In section 4, some quantum analogies of the known plaintext attack are suggested and their benefit for Eve is briefly discussed.

Journal of Modern Optics ISSN 0950–0340 print/ISSN 1362–3044 online
http://www.tandf.co.uk/journals
DOI: 10.1080/0950034021000057978

2. How to encrypt quantum information

2.1. *Quantum one-time pad*

The encryption of quantum information was independently developed in [7] and [9] and it is a generalization of a side effect of quantum teleportation [10]. Let us define the Pauli matrices as usual:

$$\sigma_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} 0 & -\mathrm{i} \\ \mathrm{i} & 0 \end{pmatrix}, \quad \sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{1}$$

When a qubit in a state ρ is teleported from Alice, then it is randomly modified by one of the Pauli operators, each with probability $\frac{1}{4}$. Since Bob (the receiver) does not know which of the operators was applied, he must obtain two classical bits from Alice to gain this knowledge. The two classical bits K specify which of the operators was applied; they determine the state of the system to be $\sigma_K \rho \sigma_K$. Without knowledge about which of the operations was applied the qubit appears to be on average in the state $\frac{1}{4}\sum_{i=0}^{3} \sigma_i \rho \sigma_i = 1/2I$ for any ρ. The state $1/2I$ contains no information about ρ and therefore this technique can be considered to be a perfect encryption of a qubit.

The encryption of one qubit follows. Let us assume that Alice wants to transmit one qubit to Bob in the way that Eve cannot use this qubit for any purpose when she intercepts it. Further let us suppose that Alice and Bob share in advance two secret classical bits K. When Alice wants to send a qubit Q in the state ρ, she performs the following: she applies the operation σ_K on Q to transform it into the state $\sigma_K \rho \sigma_K$ and sends this state to Bob via public quantum channel. Eve does not know the key, so the system appears to be in the state $1/2I$ from her point of view. On the other hand, when Bob receives the system, he applies σ_K to reconstruct the original state ρ.

The encryption of a multiple-qubit state is a simple modification of the single-qubit procedure as described above. Whenever a multiple-qubit state is factorable, we can encrypt each of the qubits independently. However the question arises of how to encrypt entangled states. Surprisingly this is done again by encrypting each qubit independently and any state ρ of n qubits will be turned into $(1/2^n)I^{\otimes n}$ (see [9] for the proof). In this way we need two classical bits to encrypt each qubit and to encrypt an n qubit state we need $2n$ bits. This encryption scheme is called the quantum one-time pad [7, 9].

2.2. *Private quantum channel*

The general framework of the quantum one time pad is called the private quantum channel and is defined in the following way (see figure 1).

Definition 1: Let $S \subseteq \mathcal{H}_{2^n}$ be a set of pure n-qubit states and $\mathcal{E} = \{p_i^{1/2} U_i\}_{i=1}^{n}$ be a superoperator, where each U_i is a unitary operator on $\mathcal{H}_{2^m}$ and $\sum_{i=1}^{N} p_i = 1$. Let ρ_a be an $(m-n)$-qubit density matrix and ρ_0 be an m-qubit density matrix. Then $[S, \mathcal{E}, \rho_a, \rho_0]$ is a *private quantum channel* if and only if for all $|\phi\rangle \in S$ it holds that

$$\mathcal{E}(|\phi\rangle\langle\phi| \otimes \rho_a) = \sum_{i=1}^{n} p_i U_i (|\phi\rangle\langle\phi| \otimes \rho_a) U_i^* = \rho_0. \tag{2}$$

The meaning of the private quantum channel is the following. Alice wants to establish a communication (quantum) channel with Bob with the property that any state $|\phi\rangle \in S$ will be transmitted securely. Eve is not able to use the transmitted

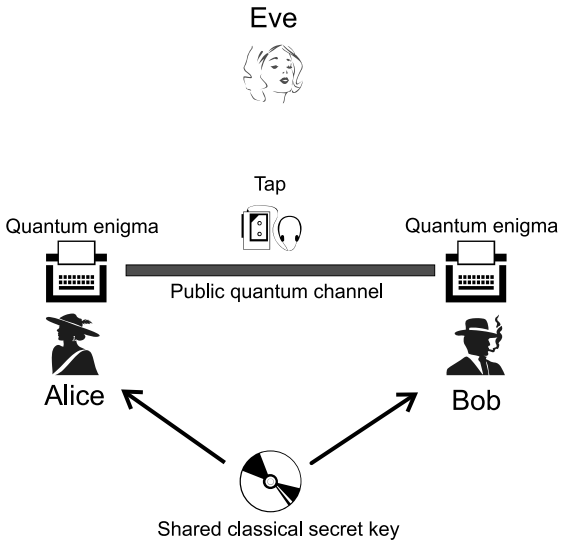

Figure 1. A schematic description of the private quantum channel.

state for any purpose. The encryption of the state is done in the way that one of the operators $\{U_i\}_i$ is applied. The operator U_i is chosen with probability p_i. The classical key specifies which of the unitary operators was applied. The unitary operators U_i are acting on $\mathcal{H}_{2^m}$, while the state $|\phi\rangle$ is only n dimensional. Therefore the unitary operator is applied on the state $|\phi\rangle\langle\phi| \otimes \rho_a$. It means that the unitary operators act on the system which is being encrypted and on the auxiliary system, which is initially factorized from the system being encrypted. The initial state of the auxiliary system is ρ_a.

The security of the transmission has the following meaning: without knowledge of the key (without knowledge about which of the operators was used) any initial state $|\phi\rangle \in S$ together with the ancilla appears to be in the state ρ_0 after the encryption. This means that all states from the set S are physically indistinguishable after the encryption.

In [7, 9] it has been shown that this method of encryption using the Pauli matrices is optimal in the sense that it is necessary to use at least two classical bits to encrypt one qubit.

2.3. *Quantum one-time pad as the private quantum channel*

We can define the quantum one-time pad described in the section 2.1 in terms of the private quantum channel framework. It serves also as an example of the private quantum channel.

The quantum one-time pad works in the way that the transmitted qubit is modified randomly by one of the Pauli operators, the corresponding key is a pair of classical bits describing which of the Pauli operators was used (there are four Pauli operators including the identity). More formally, the quantum one-time pad is $[\mathcal{H}_{2^n}, \mathcal{E}, 1/2^n I]$, where $\mathcal{E} = \{(1/2^{2n})\overline{\sigma_x} | x \in \{0,1,2,3\}^n\}$. The operator $\overline{\sigma_x}$ is a generalization of a Pauli matrix for n qubit system such that, when $x = x_1 x_2 \ldots x_n$, then $\overline{\sigma_x} = \sigma_{x_1} \otimes \sigma_{x_2} \otimes \cdots \otimes \sigma_{x_n}$.

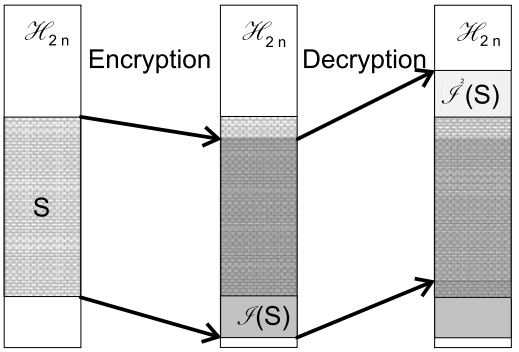

Figure 2. Relation between the sets $S, \mathcal{J}(S)$ and $\mathcal{J}^2(s)$.

3. Known-ciphertext attack

In this section we shall discuss the problem that arises from the fact that Alice sends only states from the set S and not from the whole Hilbert space. This attack must be considered whenever Eve is able to obtain any classical information about the ciphertext state. This fact especially enforces a specific usage of the classical key which is different from the usage of the key in the classical case (in the case of the classical one-time pad).

Let us define $\Im(S) = \{U_i|\phi\rangle | i = 1n, |\phi\rangle \in S\}$. The $\Im(S)$ is a set of all possible ciphertext states. Further, let $\Im^2(S) = \{U_i^*|\tilde{\phi}\rangle |\ i = 1, \ldots, n, |\tilde{\phi}\rangle \in \Im(S)\}$.

The security problem caused by the set S arises when

$$\Im^2(S) \not\subseteq S \tag{3}$$

(figure 2). When we perform decryption without knowledge of the key, we must accept all states $U_i^*|\tilde{\phi}\rangle$ as candidates for the plaintext state. However, we can safely ignore states $U_i^*|\phi\rangle$ which do not belong to the set S, we can be sure that these states were not the plaintext states. Therefore the original equation

$$\mathcal{E}^{-1}(|\tilde{\phi}\rangle\langle\tilde{\phi}|) = \sum_{i=1}^{N} p_i U_i^*|\tilde{\phi}\rangle\langle\tilde{\phi}|U_i = \rho_0 \tag{3}$$

is transformed to

$$\mathcal{E}^{-1}(|\tilde{\phi}\rangle\langle\tilde{\phi}|) = \sum_{\substack{i=1\ldots N \\ U_i^*|\tilde{\phi}\rangle \in S}} p_i U_i^*|\tilde{\phi}\rangle\langle\tilde{\phi}|U_i, \tag{5}$$

which is not equal in general to any fixed $\tilde{\rho}$. Note that $\mathcal{E}^{-1}$ is not the inverse superoperator to $\mathcal{E}$. It just describes decryption without knowledge of the key. The probabilities p_i are the same as in the case of encryption, because there is a probability p_i that $|\tilde{\phi}\rangle$ was encrypted using U_i.

Let us consider the following example: $S = \{|0\rangle, |0\rangle + |1\rangle\}$, $\mathcal{E} = \{\frac{1}{4}\sigma_i | i = 0, \ldots, 3\}, \rho_0 = 1/2I$. Therefore $\Im(S) = \{|1\rangle, |0\rangle, |0\rangle + |1\rangle, |0\rangle - |1\rangle\}$. Let us suppose that the ciphertext state is $|0\rangle + |1\rangle$. Then Eve can learn the plaintext with the probability 25% by measuring only two copies of the ciphertext state. The considered measurement basis is $\{|0\rangle, |1\rangle\}$. If the two (or more) measurements†

† In the case of two measurements the probability of obtaining different results is 50%, and the probability that Eve has chosen correct basis is 50%; this together gives us a 25% chance of success.

give the result $|0\rangle$ and $|1\rangle$, Eve can be sure that the ciphertext is neither $|0\rangle$ nor $|1\rangle$ and hence the plaintext is $|0\rangle + |1\rangle$. This is caused by the fact that $\Im^2(S) = \{|0\rangle, |1\rangle, |0\rangle + |1\rangle, |0\rangle - |1\rangle\} \not\subseteq S$. By measuring the basis $\{|0\rangle, |1\rangle\}$, we obtained the information that the ciphertext is either $|0\rangle + |1\rangle$ or $|0\rangle - |1\rangle$, which yields that the original plaintext was either $|0\rangle + |1\rangle$ or $|0\rangle - |1\rangle$. Finally, only the state $|0\rangle + |1\rangle$ is included in the set S; so we have revealed the plaintext.

If we have supposed that $|0\rangle - |1\rangle \in S$, then we would have obtained

$$\begin{aligned}\mathcal{E}^{-1}(|0\rangle + |1\rangle) &= \mathcal{E}^{-1}(|0\rangle - |1\rangle) \\ &= \tfrac{1}{2}[(|0\rangle + |1\rangle)(\langle 0| + \langle 1|) + (|0\rangle - |1\rangle)(\langle 0| - \langle 1|)] = \tfrac{1}{2}I.\end{aligned} \tag{6}$$

This is a sharp difference between our cipher and the classical one-time pad. In the classical case, Eve gains nothing when she obtains an arbitrary number of copies of ciphertext (she can even create them herself). Nevertheless, in the quantum case we encrypt a state with continuously many states using only two classical bits. This is safe as long as the classical description of the ciphertext is not known.

In this way we can define a new class of attacks which has no analogy in the classical cryptography: the *known-ciphertext attack*. This term seems to be rather strange, but we must consider the fact that in the quantum world there is a significant difference between 'to have quantum information' and 'to know quantum information' (to have a classical description of the quantum information). When Eve has the encrypted state (system in this state), she can do nothing irrespective of her abilities to manipulate with quantum information. However, when she *knows* the classical description of the encrypted state, she reduces the continuum of possible original (plaintext) states to only four possible states. This fact can in some cases allow her to determine the original state with certainty (see the previous example). In this case, knowledge of the classical description of the ciphertext leads to uncovering of the original message. This fact implies that the classical description of the ciphertext is in general confidential information as discussed in the following paragraph.

It might seem strange, but in the quantum case even the ciphertext must be kept secret in the sense that any classical information about the ciphertext must be kept secret. For example, when Alice wants to send twice the copy of a state ρ, she must use independent keys for each copy. A typical example is when the state was destroyed during transmission; Bob did not receive it and he asks Alice for a new copy. Eve knows that the transmitted information will have the same original meaning as the previous, but in the classical case this gives her no advantage. In the classical case we can send it once more using the same key (just send one more copy of the encrypted information). However, in the quantum one-time pad we must use an independent key! In this case the security is maintained and this is almost the same as teleporting an infinite number of systems in an identical state.

4. Known-plaintext attack

In the classical cryptography the known-plaintext attack is the following problem. The eavesdropper has a description of the cipher, he has the plaintext and the ciphertext. His goal is to determine the key. In the case of the classical one-

time pad the situation is simple; the eavesdropper just performs an XOR of ciphertext and plaintext and obtains the key.

In the case of our cipher the situation is similar, but we must define first the known-plaintext attack for quantum information. There are two possible (basic) definitions of the known plaintext attack. The first is that the eavesdropper has two systems P and C: the system P is in the plaintext state and the system C is in the ciphertext state. In this case the eavesdropper is not able to determine the key† (if he does not have additional information about P or C)‡. The other possibility is that the eavesdropper has a classical description of both plaintext and ciphertext. In this case he is able to determine the key and therefore we suggest that this case is considered as the known-plaintext attack in the quantum case.

Naturally, there can be a large amount of possible definitions which vary between the previous two definitions; for example the eavesdropper has some additional information about P or C, the eavesdropper has more that one copy of P or C, or the eavesdropper has classical description of P and one copy of C. The advantages given to the eavesdropper in these situations do depend on the specific realization of the private quantum channel, namely on the set S and the set of encryption operations $\{U_i\}_i$ together with the probability distribution $\{p_i\}_i$. In the case when the eavesdropper has classical description of the plaintext and one system in the ciphertext state, he is even not able to infer anything about the ciphertext.

5. Conclusion

We proposed a new type of attack which has no analogy in the classical cryptography: the known-ciphertext attack. We gave a specific example of the situation in which this type of attack applies and suggested a way to avoid it. Moreover we discussed a quantum version of the known-plaintext attack and we described a variety of situations that can be considered to be the quantum known-plaintext attack.

We point out that, each time that we design a quantum cryptographic system (protocol, cipher, etc.) we have to remember fundamental differences between the classical and quantum information. Especially important is the fact that it is impossible to obtain a partial (deterministic) information about the basic unit of classical information: the single classical bit. Either the eavesdropper knows the value of the bit or he knows nothing (certainly probabilistic description is different). In the quantum case we can have partial deterministic information about the qubit. It can be the information such as 'the state is not $|0\rangle$' or 'the state is either $|0\rangle$ or $1/2^{1/2}(|0\rangle + |1\rangle)$'. As discussed in this article, even the partial information about the plaintext can be sometimes enough to learn the plaintext. It might be interesting to investigate what partial classical information about the

† In general it is impossible even to decide whether the systems P and C are in different states.

‡ In the case of the quantum one-time pad with $S = \{|0\rangle, |1\rangle\}$ the situation is similar to the classical one-time pad. Eve measures both P and C in the basis $\{|0\rangle, |1\rangle\}$ and obtains a classical description of the plaintext and the ciphertext.

system must the eavesdropper learn to compromise the security of the (quantum) cryptographic system.

Acknowledgments

We thank Mário Ziman for helpful discussions. This work was supported by grant GACR 201/01/0413 and by the European Union projects EQUIP and QUBITS under contracts IST-1999-11053 and IST-1999-13021 respectively. V.B. would like to acknowledge an E.T.S. Walton fellowship of the Science Foundation Ireland (SFI).

References

[1] Bennett, C. H., and Brassard, G., 1984, Quantum cryptography: Public key distribution and coin tossing. *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing* (New York: IEEE), p. 175.
[2] Ekert, A. K., 1991, *Phys. Rev. Lett.*, **67,** 661.
[3] Hillery, M., Bužek, V., and Bertiaume, A., 1991, 'Quantum secret sharing.' *Phys. Rev.* A, **59,** 1829.
[4] Cleve, R., Gottesman, D., and Lo, H. K., 1999, *Phys. Rev. Lett.*, **83,** 648.
[5] Bennett, C. H., Brassard, G., Crepeau, C., and Skubiszewska, M. H., 1991, *Lecture Notes in Computer Science*, p.351.
[6] Gruska, J., 1999, *Quantum Computing* (London: McGraw-Hill).
[7] Mosca, M., Tapp, A., and de Wolf, R., 2000. quant-ph/0003101.
[8] Leung, D. W., 2002, *Quant. Info. Comp.*, **2,** 14.
[9] Boykin, P. O., and Roychowdhury, V., 2000, quant-ph/0003059.
[10] Bennett, C. H., Brassard, G., Crepeau, C., Jozsa, R., Peres, A., and Wootters, W. K., 1993, *Phys. Rev. Lett.*, **70,** 1895.