

Efficiency of the Eavesdropping in B92 QKD Protocol with a QCM

Michael Siomau¹ and Stephan Fritzsche^{2,3}

¹ Max-Planck-Institut für Kernphysik, Postfach 103980,
D-69117 Heidelberg, Germany
siomau@physi.uni-heidelberg.de

² Department of Physical Sciences, P.O. Box 3000,
Fin-90014 University of Oulu, Finland

³ Frankfurt Institute for Advanced Studies, D-60438 Frankfurt am Main, Germany

Abstract. Success of any eavesdropping attack on a quantum cryptographic protocol can be reduced by the legitimate users if they partially compare their data. It is important to know for the legitimate users what is (necessary and enough) amount of data which should be compared to ensure that (possible) illegitimate user has an arbitrary small information about the rest of data. To obtain such amount the legitimate users need to know efficiencies of all possible attacks for particular cryptographic protocol. In this work we introduce the eavesdropping attack on Bennett's B92 protocol for quantum key distribution (QKD) with a quantum cloning machine (QCM). We demonstrate efficiency of suggested attack and compare it with efficiencies of alternative attacks proposed before.

Keywords: B92 QKD protocol, QCM, mutual information, discrepancy.

1 Introduction

Security of quantum cryptography [1] implies that legitimate users (say Alice and Bob) *always* can provide such error-correction and privacy amplification codes [2] that final information of an eavesdropper (Eve) about the message transmitted from Alice to Bob is as low as it was set by legitimate users before applying the codes. During the codes realization Alice and Bob compare the values of some of their bits from the message. The rigorous problem for Alice and Bob is to construct the codes so that, from one side, the number of compared bits is minimal and, from another side, final Eve's information about the message is an arbitrary small. Thus it is important to estimate the maximal amount of information that Eve may take in an eavesdropping attack.

Efficiency of an eavesdropping attack depends from particular realization of cryptographic protocol and method of Eve's intervention. Since quantum key distribution (QKD) protocols [3]-[8] takes central place in cryptography, we pay our attention on particular QKD scheme – Bennett's B92 protocol [5]. In the B92 protocol only two nonorthogonal quantum states are utilized in order to encode

and transmit information about the cryptographic key. As usual, we suppose that information is sent from Alice to Bob by means of a quantum communication channel. At the beginning of the key distribution protocol, Alice encodes each logical bit, 0 or 1, into two nonorthogonal states, which can be parameterized as

$$\begin{aligned}
 |u\rangle &= \cos \frac{\theta}{2} |0\rangle + \sin \frac{\theta}{2} |1\rangle, \\
 |v\rangle &= \sin \frac{\theta}{2} |0\rangle + \cos \frac{\theta}{2} |1\rangle,
 \end{aligned}
 \tag{1}$$

where $|0\rangle$ and $|1\rangle$ introduce computational basis. The overlap of the states $O(\theta) \equiv |\langle u|v\rangle|^2 = \sin^2 \theta$ gives the distance between states $|u\rangle$ and $|v\rangle$ in geometric sense.

Prepared qubits (1) are sent to Bob who measures them randomly either in the standard \oplus or the diagonal \otimes basis. If, for example, Bob has chosen the standard basis \oplus and measured the state $|1\rangle$, he concludes that the state $|+\rangle$ was sent by Alice (because $|0\rangle$ state is orthogonal to measured $|1\rangle$ state). Similarly, if Bob had chosen the diagonal basis \otimes and has measured $|-\rangle$, he concludes that the state $|0\rangle$ was sent. Only this described cases are conclusive for Bob. In fact, in order to obtain the maximum information about received qubits, Bob should minimize the probability to obtain some inconclusive result. As discussed in detail by Ekert *et al.* [9], this can be achieved by a positive operator-valued measurement (POVM), and the best operators for that are

$$G_1 = \frac{1}{1 + \langle u|v\rangle} (1 - |u\rangle\langle u|), \tag{2}$$

$$G_2 = \frac{1}{1 + \langle u|v\rangle} (1 - |v\rangle\langle v|), \tag{3}$$

$$G_3 = 1 - G_1 - G_2, \tag{4}$$

where $|u\rangle$ and $|v\rangle$ denote nonorthogonal states (1) that are used in order to encode the information.

After all the qubits have been sent (and measured), Bob tells to Alice numbers of conclusive measurements via a public channel, which can be monitored but not modified by possible eavesdropper. Only those bits (obtained in Bob's conclusive measurements) can be used to construct the key, while all the rest need to be discarded because no definite conclusion can be drawn from the outcome of Bob's measurement.

Although an eavesdropping of the (quantum) communication between Alice and Bob is seriously hampered by the well-known impossibility to produce exact copies of quantum information (non-cloning theorem), the generation of approximate copies with a quantum cloning machine (QCM) [10]-[12] may enlarge the success rate for such an attack. A QCM is a device represented as unitary transformations which provides approximate copies of the input qubit states with certain fidelity

$$F = \langle \psi|\rho|\psi\rangle, \tag{5}$$

where ρ presents a density matrix of each copy and $|\psi\rangle$ is the input state. The QCM is called *symmetric* if the output states are identical to each other, and are said to be *nonsymmetric* otherwise. We restrict ourself by considering only symmetric QCM's which provides two copies from a single input state $1 \rightarrow 2$, because such QCM's provide copies with maximal fidelity in comparison with $1 \rightarrow N$ QCM's, where $N > 2$, as it was shown by Werner [13].

We always consider *individual* eavesdropping attack in which Eve interacts individually and in the same way with the qubit states traveling from Alice to Bob: Eve copies a single qubit intercepted from the communication channel, and sends one copy to Bob keeping another. Thus, in this work we consider individual eavesdropping attack on B92 protocol with symmetric ($1 \rightarrow 2$) QCM's.

The paper is organized as follows. In the next section we introduce necessary mathematical approach – discrepancy and mutual information – to describe the success of Eve within a cryptographic protocol. In section 3 we analyze efficiencies of the eavesdropping with different symmetric ($1 \rightarrow 2$) QCM's and show that meridional QCM [14] is optimal for eavesdropping in B92 protocol. In section 4 we compare efficiency of the eavesdropping with meridional QCM with efficiencies of alternative attacks discussed by Ekert *et al.* [9] and conclude that suggested eavesdropping attack is optimal for particular choice of states (1) which are used to encode information. We finish this work with conclusions.

2 Discrepancy and Mutual Information

To describe efficiency of an eavesdropping attack it is sufficient to know two values: disturbance of a qubit received by Bob and the mutual information between participants of the cryptographic protocol.

A disturbance in the transmission of the qubits can have very different reasons. Apart from an eavesdropper, the quantum control during the preparation or transmission of the qubits might be incomplete for a given realization of the quantum channel. For all practical realizations of QKD protocols, therefore, a certain error rate (discrepancy) need to be accepted, and an eavesdropper might be successful in extracting information even if the protocol is inherently secure in the ideal case. To quantify discrepancy in the transmission of a single qubit, a convenient measure is the probability that Bob detects an error. If Bob would know the state $|s\rangle$ of one or several qubits in advance, that were sent to him by Alice, he can easily test for a possible eavesdropping attack. In this case, he will receive in general the qubits no longer in a pure but a mixed state that have to be described in terms of their density matrix ρ . Then, the discrepancy that is detectable by Bob is given by

$$D = 1 - \langle s | \rho | s \rangle, \quad (6)$$

Since Bob knows the maximal discrepancy D_{max} for the given channel, he could recognize an eavesdropping attack for $D > D_{max}$ and discard the key accordingly. Later we assume, for simplicity, that the quantum control of the given

transmission is complete. With this assumption all discrepancy detected by Bob is caused by Eve.

A central question for Eve is of how much information she can extract from the transmission of the key and what is the price in terms of discrepancy. From the initial agreement between Alice and Bob about the basis states which are to be chosen randomly, Eve might know that Alice prepares the qubits in one of several states with proper probabilities. This initial agreement has to be made typically independent of a particular protocol. Before Eve has measured a given qubit, her (degree of) ignorance is given by Shannon’s entropy. After the measurement, she increased her knowledge about the system by decreasing this entropy, a measure that is called the mutual information I_{AE} that Eve has acquired about Alice’s message due to the measurement. Obviously, Eve will try to obtain as much information as possible keeping the discrepancy $D < D_{max}$.

Since Eve copy (attack) each qubit independently within B92 protocol as they are sent from Alice to Bob, as output of her cloning transformation, she then obtains two copies of one of the two possible states $\rho_{|0\rangle}$ and $\rho_{|+\rangle}$ (which just correspond to the two input states $|0\rangle$ and $|+\rangle$) with a fidelity as defined by the given QCM. While Eve transmits one of her copies further to Bob, she could measure the second copy following the same procedure as Bob.

To calculate the mutual information between Alice and Eve that is to be extracted from the eavesdropping, we can follow the procedure as described in Ref. [15]. Using the POVM elements (2)-(4), the probability for Eve to obtain the outcome μ is

$$P_{\mu i} = \text{Tr}(G_{\mu} \rho_i), \tag{7}$$

and where the operators ρ_i refer to the two possible states $\{\rho_{|0\rangle}, \rho_{|+\rangle}\}$ of her copy. After the measurement, when she has obtained a particular outcome μ , the *posterior* probability $Q_{i\mu}$ that ρ_i was prepared by Alice is

$$Q_{i\mu} = \frac{P_{\mu i} p_i}{q_{\mu}}, \tag{8}$$

where $q_{\mu} = \sum_j P_{\mu j} p_j$, and $p_j = 1/2$ is the probability for sending the states $|0\rangle$ and $|+\rangle$ within the B92 protocol. With these probabilities, the Shannon entropy (which was $H = -\log_2(1/2) = 1$ initially), becomes

$$H_{\mu} = - \sum_i Q_{i\mu} \log Q_{i\mu}, \tag{9}$$

once the result μ was obtained, and hence the mutual information is

$$I_{AE} = H - \sum_{\mu} q_{\mu} H_{\mu}. \tag{10}$$

The mutual information between Alice and Bob I_{AB} can be obtained in the same manner as it described above. In case of the eavesdropping attack with a symmetric QCM the mutual information between Alice and Bob is equal to

the mutual information between Alice and Eve $I_{AE} = I_{AB}$, since Eve and Bob receive the copies with equal fidelities.

With the help of discrepancy (6) and mutual information (10) values we may now describe efficiency of the eavesdropping in B92 QKD protocol with a QCM.

3 Optimal QCM for the Eavesdropping

QCM's have found a remarkable application in quantum cryptography, since they introduce optimal attacks for particular QKD protocols [12]. For example, *universal* QCM [10], that provides copies with constant fidelity $F = 5/6 \approx 0.83$ for an arbitrary input state, is optimal for the eavesdropping in six-state protocol [6]. Although only states from a one-dimensional subspace of original two-dimensional Hilbert state space are used to encode information in BB84 protocol [3], *equatorial* QCM [11], that realize copying of the states from the subspace with fidelity $F = 1/2 + \sqrt{1/8} \approx 0.85$, is optimal for the eavesdropping within this protocol. Obviously, optimal QCM for the eavesdropping in B92 protocol should create copies with higher fidelity than universal and equatorial QCM's for restricted set of states which covers states (1). Recently presented *meridional* QCM [14] is optimal QCM for the eavesdropping in B92 protocol, since it provides copies with fidelity

$$F(\theta) = \frac{9}{10} - \frac{1}{5} \sin^2 \theta + \frac{1}{5} \sin \theta, \quad (11)$$

for the input states $|s\rangle = \cos \frac{\theta}{2} |0\rangle + \sin \frac{\theta}{2} |1\rangle$, where $0 \leq \theta \leq \pi$. All states $|s\rangle$ belong to Eastern meridian (that includes the three states $\{|0\rangle, |1\rangle, |+\rangle\}$) of the main circle on the Bloch sphere. It is easy to see that for the input states $|s\rangle$ fidelity (11) varies a little $0.90 \leq F \leq 0.95$ and may favor this region to produce quantum copies with fidelity higher than in case of universal and equatorial quantum copying. Figure 1 displays the behavior of this fidelity for states $|s\rangle$ from Eastern meridian.

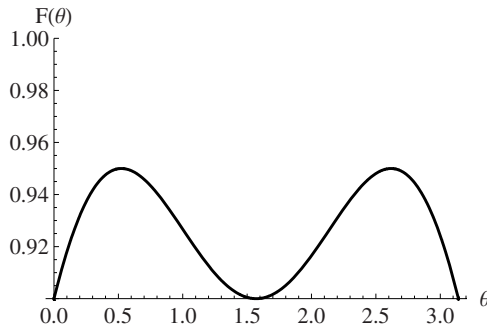


Fig. 1. Fidelity (11) of meridional QCM as function of the angle θ for the states from Eastern meridian on the Bloch sphere

4 Efficiency of the Eavesdropping with Meridional QCM

In the previous section we have shown that meridional QCM is optimal QCM for the eavesdropping in B92 protocol. With the help of definitions of the mutual information (10) and discrepancy (6) values, taking into account behavior of the fidelity function (11), we may analyze the success of Eve’s attack with meridional QCM within B92 protocol.

The mutual information between Alice and Eve as function of parameter θ of states (1) is shown at Figure 2 with solid line. The mutual information monotonically decrease from the value $I(0) = 0.5310$ (what correspond to the case when states (1) are orthogonal) to $I(\pi/2) = 0$ (when the states coincide with each other). In order to show the upper bound of information which can be achieved by Eve within B92 protocol, we also display (with dashed line) the mutual information in the case of Eve’s intervention with (unreal) ‘ideal’ QCM that provides two exact copies of the given input.

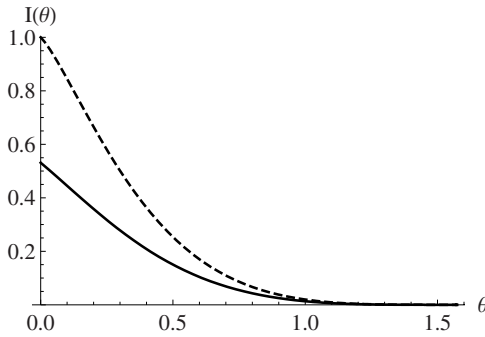


Fig. 2. This plot gives the mutual information between Alice and Eve $I(\theta)$ as function of the angle θ . Solid line introduces the mutual information in the case of Eve’s intervention with meridional QCM. Dashed line introduce unreal situation when Eve attacks the qubits with ‘ideal’ QCM.

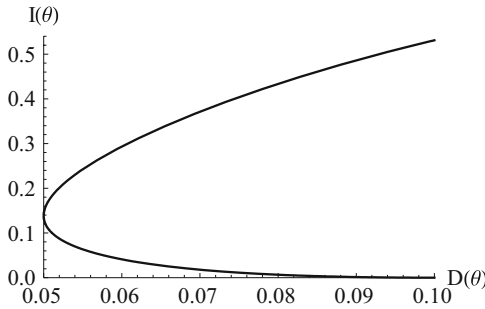


Fig. 3. This plot gives parametric dependence of the mutual information between Alice and Eve $I(\theta)$ form discrepancy $D(\theta)$. See text for further discussion.

Discrepancy $D(\theta)$ of the qubit received by Bob as function of the parameter θ of states (1) is given by equation $D(\theta) = 1 - F(\theta)$ (where $F(\theta)$ denotes the fidelity of the copy received by Bob), as it follows from definitions (5) and (6).

Having found functions $I(\theta)$ and $D(\theta)$ we present at Fig. 3 parametric dependence of the mutual information between Alice and Eve from discrepancy. The mutual information equals zero when the two states are coincide (and the overlap $O(\pi/2) = 1$). In this case Alice always prepares *one state* and sends it to Bob via communication channel. Formally, Eve introduce discrepancy $D = 0.10$ in the eavesdropping (as it follows from Eqn. (11)), but single (known) state can not be used to construct a key. With decreasing of the overlap the mutual information increases and discrepancy becomes lower due to the fidelity function (11) behavior. When the overlap between states (1) equals $O(\pi/6) = 1/4$ the mutual information is $I_{AE}(\pi/6) = 0.1384$ and discrepancy has value $D(\pi/6) = 0.05$. With further decreasing of the overlap the mutual information still increase, but discrepancy also increase.

To bring our analysis to the end we now compare efficiency of the eavesdropping with meridional QCM and efficiencies of alternative attacks proposed before [9]. In particular, Ekert *et al.* showed that *intercept-resend* attack, when Eve measures intercepted from communication channel qubit and sends to Bob qubit prepared in state $|u\rangle$ or $|v\rangle$ according to the outcome of her measurements, is optimal attack if states $|u\rangle$ and $|v\rangle$ has small overlap $O \ll 1$. In case of large overlap $O \approx 1$ the eavesdropping with *entangled probe* gives advantage for Eve to obtain maximal information about intercepted qubits causing minimal discrepancy. However, for a wide range of the overlap $0.067 \leq O \leq 0.5$, the eavesdropping with meridional QCM is more effective than both mentioned attacks. For example, if the overlap between the states $O(\pi/6) = 1/4$, discrepancy caused by Eve is $D(\pi/6) = 0.05$ and the mutual information between Alice and Eve is equal to the mutual information between Alice and Bob.

5 Conclusions

We have analyzed the eavesdropping attack on the simplest QKD scheme, where the key encoding based on two nonorthogonal quantum states, with a QCM. From this analysis, it is found that Eve, the eavesdropper, can obtain more information from meridional than from universal or equatorial QCM's causing lower disturbance to intercepted qubits. We have also demonstrated that the attack supported with meridional QCM is the most effective (i.e. optimal) attack on B92 protocol comparing to intercept-resend attack and attack with entangled probe for particular choice of the states.

Since eavesdropping attack on B92 with meridional QCM is optimal (for particular choice of the states), it introduces the maximal amount of information that Eve may take in an eavesdropping attack. Thus, obtained result should be taken into account in construction of error-correction and privacy amplification codes for B92 QKD protocol.

References

1. Lo, H.-K., Chau, H.-F.: Unconditional security of quantum key distribution over arbitrarily long distances. *Science* 283, 2050–2056 (1999); Shor, P.W., Preskill, J.: Simple proof of security of the BB84 quantum key distribution protocol. *Phys. Rev. Lett.* 85, 441–444 (2000)
2. Nielsen, M.A., Chuang, I.L.: *Quantum computation and quantum information*. Cambridge University Press, Cambridge (2000); references therein; Kilin, S.Ya., Choroshko, D.B., Nizovtsev, A.P.: *Quantum Cryptography*. Belarus science, Minsk (2007); references therein
3. Bennett, C.H., Brassard, G.: Quantum cryptography: Public key distribution and coin tossing. In: *Proceedings of IEEE International Conference on Computers, Systems and Signal Proceeding*, Bangalore, India, pp. 175–179 (1985)
4. Ekert, A.K.: Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.* 67, 661–663 (1991)
5. Bennett, C.H.: Quantum cryptography using any two nonorthogonal states. *Phys. Rev. Lett.* 68, 3121–3124 (1992)
6. Bruß, D.: Optimal eavesdropping in quantum cryptography with six states. *Phys. Rev. Lett.* 81, 3018–3021 (1998)
7. Cerf, N.J., Levy, M., Van Assche, G.: Quantum distribution of gaussian keys using squeezed states. *Phys. Rev. A* 63, 052311 (2001); Grosshans, F., Grangier, P.: Continuous variable quantum cryptography using coherent states. *Phys. Rev. Lett.* 88, 057902 (2002)
8. Scarani, V., Acin, A., Ribordy, G., Gisin, N.: Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementation. *Phys. Rev. Lett.* 92, 057901 (2004)
9. Ekert, A.K., Huttner, B., Palma, G.M., Peres, A.: Eavesdropping on quantum-cryptographical systems. *Phys. Rev. A* 50, 1047–1056 (1994)
10. Bužek, V., Hillery, M.: Quantum copying: Beyond the non-cloning theorem. *Phys. Rev. A* 54, 1844–1852 (1996)
11. Bruß, D., Cinchetti, M., D'Ariano, G.M., Macchiavello, C.: Phase covariant quantum cloning. *Phys. Rev. A* 62, 012302 (2000)
12. Scarani, V., Iblisbir, S., Gisin, N.: Quantum cloning. *Rev. Mod. Phys.* 77, 1225–1256 (2005)
13. Werner, R.F.: Optimal cloning of pure states. *Phys. Rev. A* 58, 1827–1832 (1998)
14. Siomau, M., Fritzsche, S.: High-fidelity copies from a symmetric $1 \rightarrow 2$ quantum cloning machine (2009), ArXiv:0906.1453v1
15. Peres, A.: *Quantum Theory: Concepts and Methods*. Kluwer Acad. Publ., Dordrecht (2002)