# SQL injection principle against BB84 protocol

H.Amellal, A.Meslouhi and Y. Hassouni
*Faculté des Sciences, Département de Physique,*
*LPT-URAC-13, Université Mohammed V- Agdal.*
*Av. Ibn Battouta, B.P. 1014, Rabat, Morocco*
*Email: amellal@yandex.ru*

A. El Allati
*Département de Physique*
*Faculté des Sciences et Techniques Al-Hoceima*
*Université Mohammed I - Oujda, B.P. 3, C.P. 32003 Ajdir*
*Al-Hoceima, Morocco*

***Abstract*—In order to study and analyze the security of quantum communications, we propose in this work a new quantum attack strategy alias "Malware Photon Injection Attack"(MPIA). In this attack we based on the philosophy of the classical attack "SQL Injection" and the physical properties of quantum entanglement. The effectiveness of "MPIA" is proved by the analyze of mutual information quantity variation between emitter-receiver and emitter-Eavesdropper.**

Keywords: Security; SQL injection; Quantum attacks; quantum cryptography.

## 1. Introduction

Recently, the communication security is based on different principles of quantum mechanics, such as the superposition, no cloning theorem and quantum measurement [1]. Despite that, appeared different types of quantum strategies attack, which threatening the security of quantum communication. The quantum attacks can be classified into two types: the individual attacks [2], [3] and the collective attacks [2]. Actually the attacks strategies on quantum key distribution protocols much evolved, of most important of which we find, the Intercept and Resend attack, ZLG Attack, "Photon Number Splitting Attack "(PNS), "Trojan Horse Attack" [7], Faked States Attack [8], "Time-Shift Attack" [9], "Beam Splitter Attack", and much others [2]. In the same context, to study the security of quantum communication we propose a new quantum attack "MPIA" which based on the philosophy of the classical attack "SQL Injection" and the advantages offered by the quantum Entanglement.
The paper is organized as follows: in Sect.2, Quantum Entanglement. In Sect.3 Attack strategies.In Sect.4 Security analysis, finally, a conclusion is drawn in the last section.

## 2. Attack strategies

### 2.1. Classical attack strategies

During the evolution of the cryptanalysis, there have been many types of attacks: The passive attack, the active attacks and the distributed attack. Also, a simple computer virus may hold the record for the most commonplace, recently the "SQL Injection" attack [12] considered one of the most prominent attack.
SQL is the vulnerability that results when attacking the Structured Query Language (SQL) [12]. The attacker can leverage the syntax and capabilities of SQL itself, also as the flexibility and power of underpin the database and operating system functionality available to the database, by being able to influence what is passed in the database. SQL injection is not a vulnerability that exclusively affects web applications, any code that accepts input from an unreliable source and then uses that input to form dynamic SQL statements could be vulnerable [12]. In the situation when the attack can't see

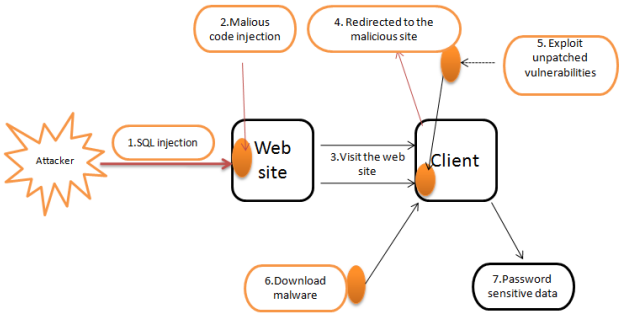


Figure 1. SQL Injection Attack Scheme.

the results in real time, when the Structured Query Language is vulnerable by the SQL injection, in this case the spy uses what called the Blind SQL injection [12]. The page with the vulnerability may not be one that displays data but will display differently depending on the results of a logical statement injected into the legitimate SQL statement called for the page. This type of attack can become time-intensive, because a new statement must be crafted for each bit recovered [12]. There are several tools that can automate this attack once the location of the vulnerability and the target information has been established.

### 2.2. Attacks Strategies On QKD protocols

The advent of the quantum communication [13], [14], [15], [24], and the evolution of the quantum key distribution protocols, especially after the entry of QKD recently the

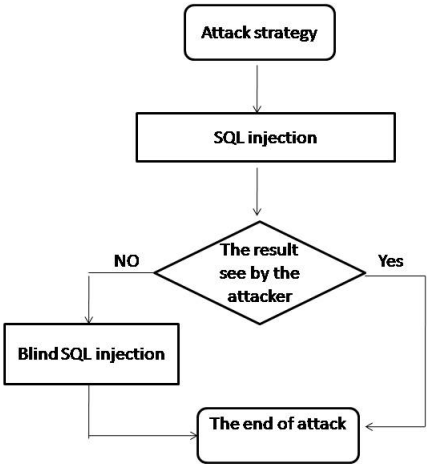


Figure 2. SQL Blind Injection Attack Algorithm

implementation phase in the modern cryptography, led to the emergence of different kind of quantum attacks strategies, under many names and classifications. The Intercept and Resend attack considered as one of the most prominent family of quantum attack strategies.

**The Intercept and Resend attack**

The intercept and resend attack considered as the intuitive type of an individual attacks strategies, in this scenario the spy tries to obtain each photon sending by Alice and measuring it in some predefined basis [2], [17]. Depending on her measurement the spy prepares a new photon and forwards it to Bob. Therefore, in the BB84 protocol, each signal is carried by a single qubit sent by Alice and received by Bob. The qubit encodes a key bit in one of the next orthonormal basis:

- When Alice uses the $V_0/V_1$ basis, her signal states will be in the following form:

$$|V_0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \quad (1)$$

$$|V_1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \quad (2)$$

- when she uses the $V_0^{'}/V_1^{'}$ basis, the signal states will have the form:

$$|V_0^{'}\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle) \quad (3)$$

$$|V_1^{'}\rangle = \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle) \quad (4)$$

We can resume the scenario of the intercept and resend attack by the following algorithm. The family of the intercept

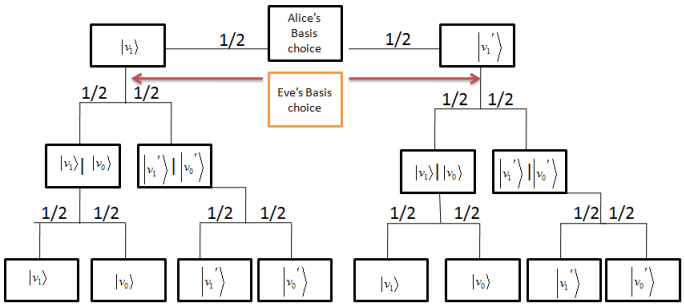


Figure 3. Intercept and Resend attack scheme.

and resend strategy contain different versions of attacks, among the most famous attacks of this family we found The faked states attack and Time-Shift Attack.

**Faked States Attack**

The Faked States Attack is one of the famous strategy attack of the Intercept and resend family, in this scenario the spy does not try to return the intercepted state, alternatively the spy prepares a signal and sends it to the receiver, which he can only uncover in a way fully controlled by the spy. In detail, the spy intercepts the signals coming from the sender using a device similar to receiver's device [2], [8], [13]. Moreover, she forwards a state to the receiver which can only be uncovered by him if he chooses the same basis as the spy. He can realize this by taking advantage of the full detector efficiency mismatch. This is a phenomenon where the signal coming into the detector has a time shift such that it is outside, the detectors sensitivity curve. Therefore, only one detector can fire and the other one is blinded out [8]. Thereby the spy can control the bit value the receiver will obtain from his measurement.

The other aim of the Faked States Attack, is to cancel the case where the receiver carry out her measurement in a basis incompatible to spy's basis, thus detecting an error. The spy can realize that by annexing a relative phase to the signal such that the whole signal is deflected to the blinded detector and is lost.

**Time-Shift Attack**

The time-shift attack strategy considered as an alternative version of the faked state attack as well benefits the detector efficiency mismatch, but unlike to the faked states attack, it is functional with the new technology, the Big variation is that the spy does not measure the state in transit between the sender and the receiver but at random shifts the time of the signal such that it arrives outside of the receiver detector sensitivity curve [2], because of her choice of the time retard, the spy is able to deduce the exact result of the receiver's measurement, which make the spy able to blind totally the detector by her time shift, he is able to gain whole information about receiver's measurement result. Further, the spy will gain only partial information about the secret key [9], [18]. In both cases, the spy never introduces any error, since she does not measure or by other words interact with the sender's state in transit.

The time-shift attack strategy Differs from the faked states attack, is that the spy has to deal with the increased loss at receiver's side in another way. Regarding the faked states attack the spy uses a brighter laser pulse to overcome the losses, with respect to the time-shift attack the spy has to replace the quantum channel by a low-loss version to compensate receiver's additional losses [18].

## 3. Description of the "MPIA" strategy

The main idea of the "MPIA" is based on the philosophy of the classical attack SQL injection, when the hacker injects the structured query language code by a malware code to obtain the information from the database, in our case in quantum environment, the attacker injects the quantum channel by a "Malware photon" using entanglement engine which makes the "malware photon" interact remotely with Alice's photon, in other words make the " malware photon" entangled with the photon sent by Alice. One of the most

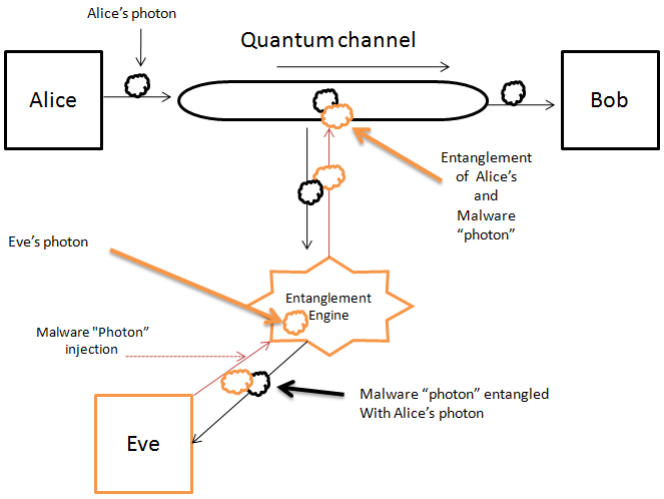


Figure 4. "Malware Photon Injection Attack" scenario

useful quantum phenomena in quantum communication in general and particularly in the quantum key distribution is the entanglement, that occurs when pairs or groups of particles are generated or interact in ways such that the quantum state of each particle cannot be described independently instead, a quantum state may be given for the system as a whole.Therefore if the spy succeeds to entangle between the "malware photon" and Alices photon, any information about the photon sent by Alice will be in his hands by a simply measure on the "malware photon".
We can resume the scenario of the "MPIA" by the following algorithm.

1) Alice sent a photon by the quantum channel.
2) Eve prepares a "malware photon" and injects it in the entanglement engine.
3) The entanglement engine injects the quantum channel by the "malware photon".
4) The entanglement engine interact remotely Alice's photon and the " malware photon".
5) Eve pulls the "malware photon" after became entangled with Alice's photon.
6) Eve Measures the " malware photon " to obtain the information about Alice's photon by exploiting advantages of quantum entanglement

## 4. Security analysis

The security level is on of the most important criteria to prove the effectiveness of any protocol. Suppose that a spy tries to intercept the information in the quantum channel (the secret key). The quantum physics proposes a set of principles and theorems as the Heisenberg uncertainty, the no-cloning theorem and the superposition, which protect at least theoretically the quantum communication against eavesdropping. Despite that, featured a set of quantum attacks that threatening the security of QKD protocols. In general we can analyse the effect of eavesdropping in different ways, in our case we based on one the variation of mutual information gain between emitter-receiver and emitter-Eavesdropper for testing the the effectiveness of the proposed attack.

Mutual information

The mutual information is a good measure for testing the level of security guaranteed by any protocol [16] by comparing the variation of information gain between emitter-receiver and emitter-Eavesdropper. Let us consider that $I_{AB}$ represent the mutual information between Alice and Bob, $I_{AE}$ represent the mutual information between Alice and Eve, x is the polarization state sent by Alice, y the state receives Bob and z the state spied Eve. The possible values of x, y and z are: x, y, $z = \{0, 1\}$.

- The mutual information between Alice and Eve.

We consider that $I_{AE}$ represent the amount of information which gain Eve from Alice, and $\alpha$ the probability that Eve chooses to measure.
In our case the "malware photon" and Alice's photon are generated in ways such that the quantum state of each photon cannot be described independently instead, that makes Eve able to disclose Alice's basis by perform a measurement on the entangled "malware photon", which means that Eve can wait until Alice reveal the used basis, and measure it in correct basis to gain all information.
We consider the four possible probabilities of measure.

$p(0|0)$:The probability that Eve measures a 0 knowing that Alice sent a 0
$p(1|0)$:The probability that Eve measures a 0 knowing that Alice sent a 0
$p(1|1)$:The probability that Eve measures a 1 knowing that Alice sent a 1
$p(0|1)$:The probability that Eve measures a 0 knowing that Alice sent a 1

For the all four possible probabilities of measure there are two cases: Eve measures the "malware photon"or Eve ignores the "malware photon".

**Eve measures the "malware photon".**

$$p(0|0) = p(1|1) = \alpha \tag{5}$$

**Eve ignores the "malware photon".**

$$p(0|0) = p(1|1) = (1-\alpha)\frac{1}{2} \tag{6}$$

where:
$1-\alpha$ is the probability that Eve chooses to ignore the "malware photon" and $\frac{1}{2}$ is the probability that Eve chooses to put a 0 in the bit string knowing that Alice sent a 1, or Eve chooses to put a 1 knowing that Alice sent a 0.
therefore:

$$p(0|0) = p(1|1) = \frac{1}{2} + \frac{\alpha}{2} \tag{7}$$

The same for $p(1|0)$ and $p(0|0)$ we have:

**If Eve measures the "malware photon".**

$$p(1|0) = p(0|1) = 0 \tag{8}$$

**If Eve ignores the "malware photon"**

$$p(1|0) = p(0|1) = (1-\alpha)\frac{1}{2} \tag{9}$$

where:
$1-\alpha$ is the probability that Eve chooses to ignore the "malware photon" and $\frac{1}{2}$ is the probability that Eve chooses to put a 0 in the bit string knowing that Alice sent a 1, or Eve chooses to put a 1 knowing that Alice sent a 0.
therefore:

$$p(0|1) = p(1|0) = \frac{1}{2} - \frac{\alpha}{2} \tag{10}$$

We can resume the upper results as:

$$\begin{array}{l} p(0|0) = p(1|1) = \frac{1}{2} + \frac{\alpha}{2} \\ p(1|0) = p(1|0) = \frac{1}{2} - \frac{\alpha}{2} \end{array} \tag{11}$$

We calculate the mutual information $I_{AE}$ by the following way :

$$\begin{aligned} I_{AE} &= \sum_{xz} P(x,z)\log_2 \frac{P(x,z)}{P(x)P(z)} \\ &= \frac{1+\alpha}{2}\log_2(1+\alpha) + \frac{1-\alpha}{2}\log_2(1-\alpha) \end{aligned} \tag{12}$$

- The mutual information between Alice and Bob

$I_{AB}$ represent the amount of information between Alice and Bob, we consider a $\alpha$ the probability that Bob chooses to measure.
The same for Bob's probabilities:

$$\begin{array}{l} p(0|0) = p(1|1) = \frac{1}{2} + \frac{\alpha}{4} \\ p(1|0) = p(0|1) = \frac{1}{2} + \frac{\alpha}{4} \end{array} \tag{13}$$

We can calculate the mutual information $I_{AB}$ by the following way:

$$\begin{aligned} I_{AB} &= \sum_{xy} P(x,y)\log_2 \frac{P(x,y)}{P(x)P(y)} \\ &= \log_2\left(2-\frac{\alpha}{2}\right) - \frac{\alpha}{4}\log_2(\frac{1}{\alpha}-1) \end{aligned} \tag{14}$$

Based on the information theory, we consider any communication protocol is secured when the legitimate receiver earns more information than the eavesdropper. In figure.5, we compare the Bob's information gain $I_{AB}$ with the rmation gain by Eve $I_{AE}$, and the difference $I_{AE} - I_{AB}$. In the

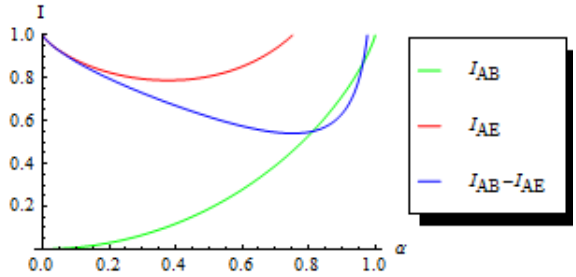


Figure 5. The mutual information quantity variation of $I_{AE}$, $I_{AB}$ and $I_{AE} - I_{AB}$ as function of $\alpha$ the probability that Eve measures the photon

Figure.5 we introduced the evolution curves of the the mutual information between Alice and Bob $I_{AB}$, the mutual information between Alice and Eve $I_{AE}$ and difference between the two mutual information $I_{AE} - I_{AB}$. From the Figure.5, it's clear that the curve of the mutual information namely $I_{AE}$ maintains height values when $\alpha \in [0, 0.8]$, contrary the mutual information namely $I_{AB}$ was low compared with the values of $I_{AE}$, that clearly appears in the values of $I_{AE} - I_{AB}$ which realize very height level when $\alpha \in [0, 0.8]$, therefore the amount of information gain by Eve much larger than the information gain by Bob which broken the security bases, and prove the effectiveness of the attack.

## 5. Conclusion

In this work, we proposed a new quantum attack on QKD protocols based on classical attack SQL injection, which is built on the injection of a malware code in the structured query language request to spy on the database. In quantum communication the database is represented by the quantum channel and the malware code represented by a "malware photon", also in the quantum environment the attacker use the advantages of quantum entanglement. In this attack Eve injects the quantum channel by a "malware photon" using the entanglement engine, which make the "malware photon" entangled with Alice's one. Therefore, Eve be able to disclose Alice's basis by perform

a measurement on the entangled ”malware photon”, and hence threat the safety of quantum communication and reduce the effectiveness of QKD protocols. Where the analyse of the variation the mutual information between emitter-receiver and emitter-Eavesdropper, we proved that Eve gain much information than Bob, which breaks the principles of communication security.

## References


[1] P.A.M.Dirac, The Principles of Quantum Mechanics, 3rd ed.Oxford: Clarendon Press (1947).

[2] C.Kollmitzer, M.Pivk, Applied quantum cryptogtraphy, Lect.Not.Phys 797,ISBN 978-3-642-04829-6, Springer(2010).

[3] E.Biham, T.Mor: Security of quantum cryptography against collective attacks. Phys. Rev.Lett.78(11), 22562259 (1997) 71.

[4] C.H.Bennett, G.Brassard: Public key distribution and coin tossing. In: Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, pp. 175179. IEEE Press, New York (1984) 71, 79, 92.

[5] C.H.Bennett, G.Brassard, S.Breidbart, S.Wiesner: Quantum Cryptography, or Unforgeable Subway Tokens. Advances in Cryptology: Proceedings of the Crypto 82, pp. 267275 (1982) 77.

[6] E.Biham, T.Mor, Security of quantum cryptography against collective attacks. Phys. Rev. Lett.78(11), 22562259 (1997) 71.

[7] V.Scarani, A.Acin, G.Ribordy and N.Gisin, Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations. Phys. Rev. Lett. 92, 057901 (2004).

[8] V.Makarov and D.R.Hjelme, Faked states attack on quantum cryptosystems. J. Mod. Opt. 52, 691705 (2005).

[9] B.Qi, C.H.F,Fung, H.K.Lo and X.Ma, Time-shift attack in practical quantum cryptosystems. Quant.Inf.Comp. 7, 7382 (2007).

[10] D.Dieks, Communication by EPR devices, Phys.Lett.A 92,6,271272 (1982).

[11] A.Ekert: Quantum cryptography based on Bell’s theorem. Phys. Rev. Lett.67(6), 661663 (1991) 71, 80.

[12] C.Justin,SQL injection attacks and defense, Syngress, MA 01803, Elsevier(2009).

[13] H. Amellal, A. Meslouhiy, Y. Hassouni and M. El Baz Quant.Inf.Process: A quantum optical firewall based on simple quantum devices 10.1007/s11128-015-1002-4.

[14] A. El Allati and M. El Baz, Opt Quant Electron, DOI 10.1007/s11082-014-9959-2.

[15] A.El Allati, Y Hassouni and N Metwally, Phys. Scr. 83 (2011) 065002.

[16] A.Meslouhi, H.Amellal, Y.Hassouni, and A.El Allati, Journal of Russian Laser Research, DOI 10.1007/s10946-014-9438-z.

[17] . E.Biham, M.Boyer, G.Brassard, J.Van de Graf, T.Mor: Security of quantum key distribution against all collective attacks. Algorithmica34(4), 372388 (2002) 71.

[18] Y.Zhao, C.H.F.Fung, B.Qi, C.Chen and H.K.Lo, Quantum hacking: experimental demonstration of time-shift attack against practical quantum-key- distribution systems. Phys. Rev. A 78, 042333 (2008).

[19] C.H.Bennett, G.Brassard, C.Crepeau, R.Jozsa, A.Peres, W.K.Wootters: Teleporting an unknown quantum state via dual classical and EPR channels. Phys. Rev. Lett.70(13), 18951899 (1993) 79

[20] D.Bruss: Optimal eavesdropping in quantum cryptography with six states. Phys. Rev. Lett.81(14), 30183021 (1998) 71.

[21] W.Y.Hwang, Quantum key distribution with high loss:Toward global secure communication. Phys. Rev. Lett.91, 057901 (2003).

[22] P.W.Shor, and J.Preskill, Simple proof of security of the BB84 quantum key distribution protocol. Phys.Rev.Lett. 85, 441444 (2000)

[23] S.Bose, V.Vedral, P.L.Knight, Multiparticle generalization of entanglement swapping.Phys.Rev.A57(2), 822829 (1998) 81.

[24] A.El Allati, M.El Baz, and Y. Hassouni, Quant.Inf.Process. 10 (2011) 589.