QCrypt 2013
3rd annual conference on quantum cryptography

QUANTUM FLOWS FOR SECRET KEY DISTRIBUTION

LUIS A. LIZAMA-PÉREZ
J. MAURICIO LÓPEZ
EDUARDO DE CARLOS LÓPEZ

In practice, the security of a Quantum Key Distribution (QKD) system relies not only on quantum mechanical principles, but it also significantly relies on the physical implementation of the protocol. Nowadays, technological detector loopholes of QKD systems have been demonstrated, and some successful attacks that exploit vulnerabilities of the Avalanche Photo Diodes (APD's) have been performed. The ideal quantum scenario has been continuously reduced, thus requiring to enhance QKD to more general protocols that can be device-independent. Recently, it has been shown that faked states attack works successfully on widely used QKD protocols, namely $BB84$, $SARG04$, phase-time, $DPSK$, Ekert protocol and the decoy method.

In the QKD protocols published so far, it is defined a single photonic gain because there is an unique qubit class that is used to construct the photonic quantum flow that goes from Alice to Bob. Frequently, the security of a protocol is based on its capability to detect deviations in the photonic gain of the quantum flow in presence of Eve. In contrast, in the $ack-QKD$ protocol, we use two different quantum flows, each one using a multi-qubit state. The multi-qubit is formed by two qubits, so we call it a bi-qubit state. These bi-qubits are chosen in such a way that they are $non-orthogonal$ or $parallel$ states.

Let us summarize briefly the $ack-QKD$ protocol:

Consider a $BB84$ based protocol that encodes a classical bit using the four non-orthogonal quantum states: X_0, X_1, Z_0 and Z_1. In contrast, in the $ack-QKD$ protocol Alice codifies one classical bit using two quantum states. To distill one secret bit Alice sends two consecutive pulses to Bob who measures them using the same basis measurement (X or Z). In the protocol, such pair of pulses can be $non-orthogonal$ states: $(X_0, Z_0), (X_0, Z_1), (X_1, Z_0), (X_1, Z_1)$ or $parallel$ states: $(X_0, X_0), (Z_0, Z_0), (X_1, X_1), (Z_1, Z_1)$. Alice chooses randomly between sending $parallel$ or $non-orthogonal$ states. We argue that the following statements are true:

1. By using pairs of quantum states two different detection events are produced: single detection events and double detection events. This in turn implies that two photonic gains are generated: The gain of the single detection events and the gain of the double detection events, each one composed by $parallel$ and $non-orthogonal$ states at random.
2. It can be shown that the photonic gain of single and double detection events is different each other for any specific parameters of the QKD system.

3. The *parallel* and $non-orthogonal$ quantum states cannot be discriminated under the usual basis measurement at Bob's (or Eve's) side.
4. In presence of the intercept-resend with faked states the eavesdropper is obligated to adjust the two photonic gains; otherwise she will be detected in the channel. However, it should be noticed that only Alice can verify each photonic gain, the *parallel* and the $non-orthogonal$ because she uses the matching cases (publicly announced) of the *parallel* and $non-orthogonal$ states to verify such gains.
5. Since the *parallel* and $non - orthogonal$ states are randomly interleaved and they are indistinguishable under quantum basis measurement, the eavesdropper is obligated to adjust randomly the two photonic gains. Therefore she increases the error rate of the protocol.

In Figure 1a) is represented the $non-orthogonal$ bi-qubit. One of the two states always matches either basis measurement but the other state behaves probabilistically (the order of states can be inverted and the argument holds). The second bi-qubit (see Figure 1b)) uses *orthogonal* states which produce ambiguous results after measurement no matter the basis Bob chooses. For this reason *orthogonal* states cannot be used in the protocol and we ignore them. The last bi-qubit (Figure 1c)) is formed by two identical (or *parallel*) states and they produce a matching measurement provided Bob chooses the compatible basis measurement. Since Bob's matching measurements occur half of the times, the sifting ratio of the *parallel* detection events is the same as the $non - orthogonal$ case.

Each time Bob's measures a bi-qubit sent by Alice, one of the following possible detection events can be obtained:

i)The states produce a double detection event. We use the symbol $(+,+)$ to denote the photonic gain of the double detection event. This event can be of two types: if the detection events are registered in the same detector then we have a double matching $(2M)$ detection event. Otherwise, if the measurement of the states yields opposite results then we have a double non-matching $(2nM)$ detection event. While $(2M)$ results are useful to distill secret bits, the $(2nM)$ results are useless and must be discarded [b].
In a lossy channel there are two more possible outcomes:
ii)The single detection event, which occurs when Bob obtains only one detection event because the other state is lost. We use the symbol $(\pm,\mp)$ to denote the single detection event. To be more specific Bob will use the symbol $(S$-$i)$ to represent the single detection event, where i can be 1 or 2, depending of the state-number that gives a click after he applies the basis measurement X or Z to the two consecutive incoming states. Thus, the number i will be announced publicly by Bob.

[b] In the $(2M)$ detection event we say that the second measurement is the acknowledgment (the *ack*) of the first measurement.

iii) The two pulses are lost. This case is represented with the symbol $(-,-)$ or alternatively as $2L$.

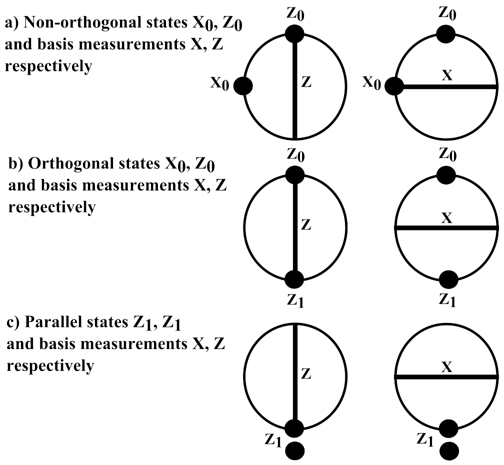
a) Non-orthogonal states X0, Z0
and basis measurements X, Z
respectively
Z0
X0
Z
Z0
X0
X
b) Orthogonal states X0, Z0
and basis measurements X, Z
respectively
Z0
Z
Z1
Z0
X
Z1
c) Parallel states Z1, Z1
and basis measurements X, Z
respectively
Z
Z1
X
Z1

Fig. 1. The qubits are represented as black dots in the bi-dimensional Bloch sphere. In a) the $non-orthogonal$ states are right-angled in the sphere, in b) the $orthogonal$ states are drawn diametrically opposed and in c) the identical (or $parallel$) states occupy the same place in the sphere. The basis measurement X and Z are depicted as horizontal and vertical lines, respectively.

In the $ack-QKD$ protocol, Alice and Bob use two consecutive states, $parallel$ or $non-orthogonal$ to distill one secret bit. Provided the measurement produces a double detection event ($2M$), Bob obtains the secret bit from the detector-bit that produces the double detection event. At Alice's side she obtains the secret bit from the bit that was codified into the two consecutive $parallel$ states. However, if such detection comes from $non-orthogonal$ states Alice discards the state-bit that is incompatible with the announced basis measurement. By contrast, she obtains the secret bit from the state-bit that is compatible with the basis measurement. They also distill a secret bit from $parallel$ and $non-orthogonal$ single matching detection events. This case corresponds to the usual compatible basis measurement as in the $BB84$ which implies that one of the two states prepared by Alice is lost but the other is detected and matches the basis measurement chosen by Bob. Finally, they discard the remaining cases and they proceed to perform the error correction algorithm of the key distillation process, as usually in QKD.

The $ack-QKD$ protocol resists a number of attacks such as the intercept-resend attack with faked states, the insertion attack without intercept-resend and the Photon Number Splitting (PNS) attack. The $ack-QKD$ protocol does not require additional hardware other than the $BB84$ protocol hardware and it can be implemented at the high level as a software application.