Using MACROBITS to illustrate the logic of quantum cryptography protocols

J. A. M. Pereira

Departamento de Física. UNIRIO, Rio de Janeiro, Brasil

Abstract. Quantum information requires a different way of thinking and sets a challenge to science education. One amazing characteristic of quantum algorithms is to deliver results with 100% certainty despite the probabilistic nature of quantum mechanics in which they are based on. In the proposed workshop, two educational routines based on quantum cryptography protocols (BB84 and Ek91) are presented as a hands-on activity. The procedures use tokens called MACROBITS and are designed so the logic involved in quantum key distribution can be grasped by the audience. The workshop aims to perform a transmission of a short message between two participants.

Introduction

The field of quantum information is a growing research area that has overcome technical difficulties, both theoretical and experimental, over the past few decades. Among the related applications, quantum cryptography methods begun to pop-up in the 80´s and today there are two well established methods for key distribution: the BB84 protocol, which is based on the measurement of prepared states [1] and the Ek91, which is based on entanglement [2]. It is worth mention that quantum measurements return certain results in these two situations. In both cases, arrays of q-bits are exchanged between the participants permitting the construction of a sequence of bits that can be used to encrypt messages.

In this workshop, two educational routines are presented step-by-step to emulate quantum cryptography protocols (BB84 and Ek91). The procedures use a tool we have developed and called MACROBIT (M-bit) as a mean to imitate the logic of quantum key distribution algorithms [3].

Methods

The M-bit is a classical object in the scale of centimetres, shaped in such a way that it can be classified by two distinct properties (fig. 1). They can be crafted using common materials such as PVC tubes, plaster and coloured tape. It consists of a right round cylinder painted in two different colors (figure 1).

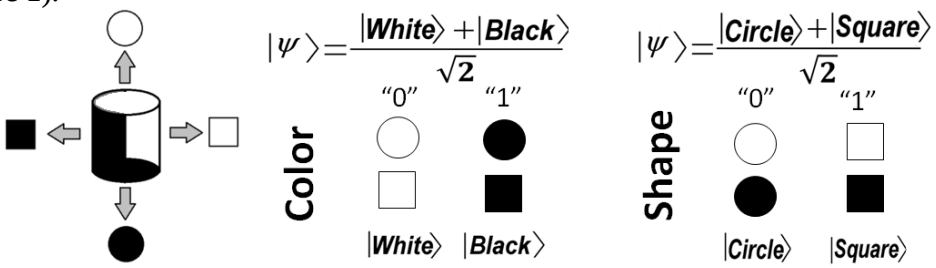

Fig. 1. Four possible side views of one M-bit. The M-bit "state vector" can be written in two different basis.

As seen in figure 1, from left to right, the M-bit can be characterized by its side views according to its colour (black or white) or to its shape (circle or square). This permits to represent the binary values "0" or "1" using two different criteria which introduces an important and useful ambiguity in regard to a binary representation.

The proposed hands-on activities are based on the interpretation of M-bits arrays, such as the one shown in figure 2, that can be translated into a binary sequence using suitable criteria.

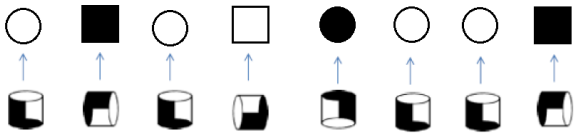

Fig. 2. An array of 8 M-bits and their corresponding read-outs. The attribution of the binary values "0" and "1" depends on the criterion the participants use.

BB84 routine

In the BB84 routine two participants (emitter and receiver) can simulate the so called sifting procedure. The emitter prepares an array of M-bits taking note of the criterion (color or shape) in which he organizes the set and sends it to the receiver. In his turn, the receiver read-out the M-bits according to his own criterion. The final step to produce the cryptographic key is the comparison between the criteria used by each participant. The key is formed by selecting the results through a sifting process. The M-bit read-outs are kept in the array if the receiver use the same criteria as prepared by the emitter, thus emulating the measurement of a prepared quantum state.

Ek91 routine

In the EK91 routine a third participant and two arrays of M-bits are required. This third partner is the entangler. He prepares two arrays of M-bits taking the same criterion to set-up each pair (if the chosen criterion is color, the entangler puts together two white shapes for instance). That means the two arrays are correlated (thus emulating the entanglement). He sends one array to the emitter and the correlated one to the receiver. Both partners make their read-outs and if they choose the same criterion as the entangler, they will be sure that their results are the same and form the key using these results.

Conclusion

Cryptography requires a few steps such as coding a message in a binary sequence, producing a encrypting key and transmitting the encrypted message. After finishing the production of the key, either by de BB84 or by Ek91, the emitter encrypts the message and send it to the receiver. The final step of the hands-on activity is the decryption by the receiver. These procedures are explained during the workshop.

Presenting the conceptual framework of quantum mechanics to students and the logic of the quantum mechanical way of thinking are some benefits of using the MACROBITS. Although, it is necessary to stress that M-bits are classical objects and there are crucial differences that have to be addressed: the M-bits are not destroyed because of the measurement as it happens to a q-bit, so there is no state vector collapse and the correlations between M-bits are always of classical nature.

References

[1] C. H. Bennett and G. Brassard, *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing vol. 175*, New York, 1984.

[2] A. K. Ekert, *Phys. Rev. Lett*. **67**(6) (1991) 661–663.

[3] F. Damaceno, *Inserindo Elementos da Criptografia Quântica no Ensino Médio*, Master dissertation, UNIRIO, Rio de Janeiro, Brasil (2019) - supervisor J. A. M. Pereira.