MACROBITS, a teaching tool for quantum cryptography

J. A. M. Pereira, F. Damaceno.

Departamento de Física. UNIRIO, Rio de Janeiro, Brasil

Abstract

One amazing characteristic of quantum algorithms is how they can deliver results with 100% certainty despite their structure being based on the probabilistic interpretation of quantum mechanics. This type of algorithm requires a different way of thinking and sets a challenge for science educators. A routine to emulate quantum cryptography protocols for high school students is proposed in this work. The educational procedure uses a tool we have developed and called MACROBIT as a mean to mimic algorithms of quantum key distribution. The MACROBITS are useful to illustrate quantum mechanics concepts such as superposition, change of basis and quantum measurement.

Introduction

Quantum cryptography is a branch quantum information. It is a growing research field that had overcome technical difficulties, both theoretical and experimental, over the past few decades. The idea of building a quantum computer, for instance, is attributed to R. Feynmann during a seminar in 1981 [1]. The main issue was to discuss the impossibility of using classical computers to simulate quantum mechanical problems due to the intrinsic probabilistic character of the quantum theory. The smallest information unit in quantum information is nowadays called the q-bit, a term that appeared in 1995 in a paper by B. Schumacher [2]. Cryptographic methods based on Quantum properties begun to pop-up in the 80´s when Bennet and Brassard first presented the BB84 protocol, which is based on quantum superposition in different basis and in quantum measurements [3]. Another important work is due to A. Ekert who developed the EK91 protocol which uses another characteristic of quantum mechanics: entanglement [4].

The development of quantum mechanics required major paradigm shifts and still causes perplexity, even for experienced physicists. Nevertheless, the necessary effort has been done in order to bring quantum physics concepts to the secondary education audience [5,6]. In the present work, the development of a toy game that can be manipulated by the students is reported. They are invited to produce a cryptographic key, in order to exchange a secret message using tokens called MACROBITS. In the process, they get in touch with quantum concepts and can see how sure results can be obtained even using the probabilistic methods of quantum theory [7].

Methods

Cryptography requires a few steps such as encoding a message in a binary sequence, producing a encrypting key and transmitting the encrypted message. Quantum mechanics is useful in two aspects: the construction of a random sequence of bits, which represents the encrypting key, and the security of the key transmission process. By MACROBIT (M-bit) we stand for an object in the scale of centimeters, shaped in such a way that it can be classified by two distinct properties. At the same time, it introduces a useful ambiguity in regard to a binary representation. The M-bits were

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).

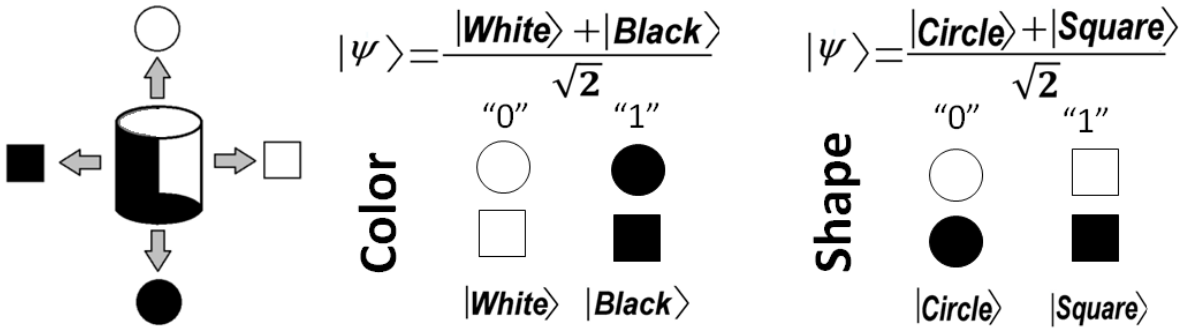

Fig. 1. Four possible side views of one M-bit. The M-bit "state vector" can be written in two different basis.

As seen in figure 1, the M-bit can be characterized by its side views according to its shape (circle or square) or colour (black or white). This permits to represent the binary values "0" or "1" in two different basis introducing a useful ambiguity that makes possible the link of the game with cryptographic protocols. The sifting procedure in BB84 protocol can be easily replicated with a set of M-bits for instance. The emitter prepares a set of M-bits, taking note of the basis in which he organizes the set. He hides them inside a blackboard box eraser and sends to a receiver. In his turn, the receiver opens the box and measure the M-bits according to his own set of basis. The final step to produce the cryptographic key is the comparison between the set of basis used by each participant. The results to be kept in the sifting process are the ones in which the M-bit was measured by the receiver in the same basis as it was prepared by the emitter (see next section). Since there is a 50% chance that the receiver chooses the same basis the emitter chose to prepare the M-bit, nearly half of the sequence will be discarded. This brings the possibility to detect a spy since if the message is intercepted and resend by a third party the frequency of errors would increase to 75%.

Application

As an example one could use a four-character alphabet, like a genomic sequence composed by the letters G C T A, to illustrate the usage of a M-bit sequence. A sentence like C C G T for instance could be encoded by one M-byte like 10 10 11 01 (where G = 11, C = 10, T=01 and A = 00). The next step is to create a random sequence of 0´s and 1´s to serve as a seed to create the encrypting key. The roll of a dice or a simple coin toss could be used for this purpose. Let us say the seed sequence is 1000 1100 0101 0011 (there are 16 characters since the expected error rate is 50% as seen in the previous section). The player that will send the message must now represent the seed sequence using the M-bits. In order to do that, he needs to choose what criteria must be used to define each M-bit representing the seed. The fist character of the seed random sequence is a 1 so if the criterion to define the first M-bit is color it will be represented by a black figure regardless of its shape (see figure 1). The second bit of the seed sequence is a 0 and the player can choose a different criterion to define the second M-bit. If this criterion is shape the second M-bit is represented by a circle irrespective to its color. Figure 2a shows the seed sequence followed by possible choices for the criteria on 2b (c for color and s for shape). The array of M-bits corresponding to the key is shown in 2c. In the language of quantum mechanics one say that a sequence of 16 q-bit states was prepared by the emitter. The M-bits are then arranged in a way to replicate figure 2c and this is sent

to the message receiver. In its turn, the receiver will choose how he will read the M-bits in an independent way. He could use the sequence shown in 2d for instance. After reading all 16 M-bits the players start the sifting process which consists of checking the cases where the two players choose the same criterion to prepare and read a given M-bit. In other words, the measurement made by the receiver is accepted as correct by both players whenever line 2b coincides with line 2d. In quantum mechanics one say that the measurement was made in the same basis in which the state was prepared hence the match between the emitter and the receiver will happen.

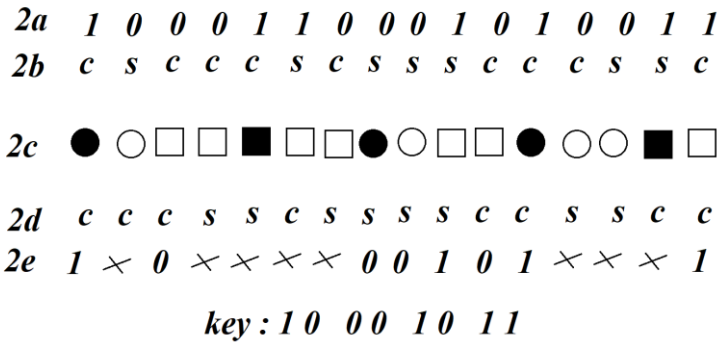

Fig. 2 – (a) A random sequence of bits. (b) Criteria used to set the M-bit array (c is for color, s is for shape) (c) The M-bit array prepared by the emitter (d) Criteria used by the receiver to read the M-bit array (e) Resulting sequence after the sifting procedure. The encrypting key is 10001011.

The seed sequence is reduced to the 8 bits necessary to the encrypting procedure. The emitter has just to binary add bit by bit the message to the key (following the binary addition rules 0 + 0 = 1 + 1 = 0, 0 + 1= 1 + 0 = 1) and the decrypting procedure is just repeating the binary addition by the receiver.

Conclusion

The M-bits showed its usefulness to introduce quantum concepts behind cryptographic protocols such as superposition of states, change of basis and quantum measurement. Although, some goals can be achieved with them it is necessary to stress that M-bits are classical objects and there are crucial differences that have to be addressed. The most important is that the M-bit is not destroyed because of the measurement as it happens to a q-bit, so there is no state vector collapse in the M-bit case.

References

[1] Richard P Feynman. *Simulating physics with computers*, 1981. International Journal of Theoretical Physics, 21(6/7).
[2] B. Shumacher, Phys. Rev. A 51 (a) (1995) 2738
[3] C. H. Bennett and G. Brassard. Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, volume 175, page 8. New York, 1984.
[4] Ekert, Artur K. (5 August 1991). Phys. Rev. Lett. 67 (6): 661–663.
[5] B. Jarosievitz; C. Sükösd, *Teaching-learning Contemporary Physics: From Research to Practice, Challenges in physics education*, ISSN 2662-8430
[6] M. LeBellac, *An Introduction to the quantum world*, World Scientific, ISBN 978-9814522427.

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