UNIVERSIDADE FEDERAL DO ESTADO DO RIO DE JANEIRO

MESTRADO NACIONAL PROFISSIONAL EM ENSINO DE FÍSICA

Aluno:

Fabrício Damasceno Belisário

Orientador:

João Alberto Mesquita Pereira

Inserindo Elementos da Criptografia Quântica no Ensino Médio

RESUMO

Por meio de um jogo, pretendemos apresentar uma proposta para o ensino de mecânica quântica no ensino básico. Utilizando o conceito da polarização do fóton, queremos familiarizar os alunos com conceitos relevantes próprios da física quântica. O jogo usa como pano de fundo o protocolo BB84, em que os participantes devem seguir os passos propostos no protocolo para transmitir uma informação de modo seguro.

Palavras-chave: Mecânica Quântica. Polarização do Fóton. Protocolo BB84. Ensino Básico.

ABSTRACT

By means of a game we intend to present a proposal for the teaching of quantum mechanics at basic education level. We focus on the concept of photon polarization as we want to familiarize students with relevant concepts in quantum physics. The game uses the BB84 protocol as a background. Participants must follow the protocol steps to transmit information in a secure way.

Keywords: Quantum Mechanics. Photon Polarization. BB84 Protocol. Basic Education

AGRADECIMENTOS

Agradeço especialmente a minha família e amigos que sempre foram base, alicerce e companhia durante toda e todas as caminhadas.

Agradeço também aos colegas e professores do MNPEF que foram fundamentais durante todo o processo de formação.

O ingresso no Mestrado Nacional Profissional em Ensino de Física me fez olhar a educação e a Física de forma mais ampla e em comum uma com a outra. Pude perceber que existem inúmeras possibilidades de transmitir conhecimento criando novas alternativas, fazendo dessa atividade uma jornada prazerosa que nos desafia a pensar em um lugar fora do comum. Produzir um novo produto foi uma tarefa que chegou até a mim através do mestrado me exigindo um desempenho que me trouxe mais conhecimento e crescimento nunca antes atingido. Enfim, a experiência do mestrado nacional aprimorou, de fato, algumas das minhas concepções sobre o ensino de Física na modernidade.

Minha proposta inicial de produto para o mestrado era de desenvolver novas práticas experimentais que pudessem reproduzir fenômenos que ocorriam na natureza em um ambiente controlado e de acesso aos alunos. Porém, fui apresentado ao meu então orientador João Pereira que me sugeriu a ideia de fazermos o meu produto abordando a Mecânica Quântica e mais precisamente o tema da criptografia quântica incluindo a concepção dos macrobits. Resolvi aceitar o tema sugerido o que resultou em um enriquecimento do meu repertório didático e ainda trazer para a sala de aula um assunto inédito. Essa inserção veio através de uma espécie de jogo que pudesse representar simulações do mundo quântico e esse jogo poderia ser utilizado por qualquer professor de física para introduzir alunos da educação básica nesse universo tão desconhecido pela grande maioria. O percurso do desenvolvimento do produto foi uma "aprendizagem ativa", na melhor acepção do conceito. Ainda devo agradecimentos a meu orientador na redação / revisão da dissertação e especialmente dos capítulos 3 e 4.

Ainda agradeço aos meus alunos que concordaram em participar desta nova experiência didática, colegas com quem compartilhei as novidades e ideias que foram surgindo ao longo do trabalho.

SUMÁRIO

CAPÍTULO 1

Introdução

1.1- Apresentando o problema

O presente trabalho tem o objetivo de apresentar uma proposta para o ensino de física quântica no ensino básico, aproveitando o conceito da polarização do fóton para introduzir alguns conceitos relevantes próprios da física quântica. Mais especificamente, pretende-se abordar o protocolo BB84, de criptografia quântica, na forma de um jogo em que os participantes devem seguir os passos propostos no protocolo para transmitir uma informação de modo seguro. Diversos autores apontam benefícios na inserção de assuntos pertinentes à Física Moderna no ensino médio.

> "A pesquisa em Física induz a um Ensino de Física que deva, a princípio, ser sua própria imagem e semelhança. A partir disso, idéias, conceitos, teorias são, então, transpostos para os programas escolares e materiais didáticos."
> (Brockington,G. e Pietrocola,M.USP,2005.387-409p.)

Entre esses benefícios, pode ser citado o aproveitamento de um interesse latente que os estudantes porventura tenham a respeito do assunto, já que a criptografia quântica é algo presente nos meios de comunicação e em revistas de divulgação a que os alunos têm acesso. Essa inserção contempla o segundo ano do ensino médio, onde é tratada a Óptica, o que pode também ser visto como uma justificativa para o aprendizado das propriedades da luz.

À abordagem da física quântica proposta neste trabalho, soma-se uma linguagem tecnológica muito utilizada no campo da programação digital, que é também usada na Criptografia: o código binário. E junto a ela, uma recente modelagem criptográfica que utiliza a física quântica: a Criptografia Quântica. Essa abordagem é feita de forma que os alunos possam entender a finalidade da criptografia e ainda aprender elementos da Física Quântica. Esta dissertação poderá ser utilizada por qualquer professor do ensino básico para a abordagem do assunto. As duas principais ideias da mecânica quântica que estão presentes no jogo são a da superposição de estados e a do colapso do vetor de

estado (ou colapso da função de onda). Para tanto, o jogo utiliza-se de peças denominadas 'macrobits', que têm a função de simular o comportamento quântico de fótons, por exemplo.

Do ponto de vista pedagógico, o tratamento dado ao desenvolvimento do jogo, segue, ao menos em parte, as ideias da aprendizagem significativa. O que se pretende é que o jogo sirva como instrumento para inserir conteúdos e vocabulário pertinentes à mecânica quântica na estrutura cognitiva dos alunos. Na linguagem da aprendizagem significativa de Ausubel, diz-se que o jogo tem o objetivo de introduzir subsunçores que possam alicerçar o estudo mais aprofundado da mecânica quântica, ou seja, ele funciona como um organizador prévio.

> "Novas ideias e informações podem ser aprendidas e retidas na medida em que conceitos, ideias ou proposições relevantes e inclusivos estejam adequadamente claros e disponíveis na estrutura cognitiva do indivíduo e funcionem, dessa forma, como "ancoradouro" para novas ideias, conceitos ou proposições."
> (Ausubel apud Moreira,A.M. São Paulo. 2014. Cap 11)

Além disso, com a incorporação das regras do jogo, da funcionalidade de suas peças, acessórios e tabelas, as quais "concretizam" as ideias da mecânica quântica no produto, os alunos podem, ao menos em princípio, desenvolver uma maneira de pensar que envolva os conceitos da Mecânica Quântica. Pode-se dizer ainda, que as ações pretendidas na implementação do jogo seguem as ideias da aprendizagem ativa, no sentido de que a atividade proposta requer maior interação com o algoritmo do jogo do que com o quadro negro. Assim, o aluno tem maior participação, estando mais envolvido nas atividades com seus pares com um caráter mais explorador e recebe feedback do seu professor no momento em que aprende.

Em resumo, o que se pretende com esse trabalho é apresentar um dispositivo didático que seja capaz de estabelecer na estrutura cognitiva do aprendiz alguns conceitos-chave da teoria quântica e de uma de suas aplicações relevantes nos dias atuais.

1.2 – Métodos Criptográficos

No ano de 1984, os cientistas Charles H Bennet e Gilles Brassard apresentaram em uma conferência sobre ciência da computação, na Índia, uma maneira de encriptar mensagens utilizando métodos próprios da mecânica quântica. O protocolo por eles

criado ficou conhecido como BB84 (de Bennet - Brassard e o ano 1984). Logo no resumo do trabalho fala-se sobre as vantagens do uso de propriedades físicas de sistemas quânticos simples, como a polarização do fóton, para o ramo da criptografia. O princípio da incerteza é apontado como sendo a fonte de um método seguro para a distribuição de chaves criptográficas. Os métodos clássicos de criptografia, tais como o disco de césar, a ENIGMA e mais recentemente o RSA, carecem desta característica, o que os torna vulneráveis. O RSA (devido às iniciais dos sobrenomes dos seus criadores; Ron Rivest, Adi Shamir e Leonard Adleman) é um método matemático de criptografia baseado na dificuldade da fatoração de números primos. Porém com o avanço dos computadores e seus processadores cada vez mais rápidos, o RSA apresenta maior vulnerabilidade, em comparação com a criptografia quântica, que apresentaremos nesse trabalho. A título de curiosidade, é notável a citação ao protocolo BB84 que aparece no cinema, já que um dos personagens robóticos de uma conhecida série possui o nome BB8 (figura 1.1) em clara alusão ao protocolo que será trabalhado nesta dissertação.

figura 1.1 – BB8, personagem robótico da sequência de filmes Star Wars.

1.3 - Escopo do trabalho

O capítulo 2 traz a conceituação do problema da criptografia com alguns exemplos e introduzir questionamentos pertinentes ao produto.

O capítulo 3 oferece uma descrição sobre os aspectos do trabalho ligados à Mecânica Quântica. Inclui-se aqui a parte da Ótica que é relevante para operacionalizar o algoritmo de criptografia.

O capítulo 4 contém as etapas da confecção do produto, materiais utilizados, apresenta cada parte que compõe o jogo e suas definições.

O capítulo 5 aponta a aplicação do produto em sala de aula, como foi apresentado o jogo aos alunos, a dinâmica e a evolução do jogo até o momento que a mensagem é revelada.

O capítulo 6 apresenta os resultados obtidos por meio de um questionário ao qual alunos foram submetidos para que se tenha uma ideia de se o objetivo educacional pretendido foi atingido.

Há ainda alguns apêndices onde são definidas as regras do jogo, apresentação das cartelas usadas no jogo, o questionário aplicado aos alunos e algumas das respostas dos alunos.

CAPÍTULO 2

CRIPTOGRAFIA

2.1 – Conceituação

A criptografia é uma técnica para transmitir informações de uma forma oculta, ou seja, uma forma segura de se comunicar ou enviar dados sem que o seu conteúdo seja descoberto por outros que não aqueles que deveriam receber as informações. Um exemplo simples de uma mensagem criptografada utilizando o próprio alfabeto como fonte criptográfica pode ser seguido abaixo. Digamos que se deseje criptografar a seguinte linha:

mestradonacionalprofissionalemensinodefisica (2.1)

1- Criamos uma sequência diferente do alfabeto. Neste caso invertemos a ordem sequencial das letras do alfabeto (conforme a segunda linha da tabela 2.1):

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
z	y	x	w	v	u	t	s	r	q	p	o	n	m	l	k	j	i	h	g	f	e	d	c	b	a

Tabela 2.1 – A primeira linha é o alfabeto na sua sequência normal, já a segunda linha é o alfabeto com sua sequência invertida onde cada letra será usada no lugar da letra da primeira linha.

2- Escrevemos a mensagem que queremos usando as letras relativas à nova sequência criada (substituindo as letras da mensagem original pela correspondente na segunda linha):

nvhgizwlmzxrlmzokilurhhrlmzovnvmhrmlwvurhrxz (2.2)

3- Enviamos a mensagem criptografada.

4- O receptor necessita ter a “chave” para “descriptografar” a mensagem enviada. Ou seja, ele precisa conhecer o mecanismo usado para fazer a correspondência entre a mensagem original e a mensagem criptografada. Ao saber que as letras

do alfabeto foram usadas com a correspondência invertida, o receptor poderá ler a real mensagem que lhe foi enviada.

Não é de hoje que técnicas como essa são usadas com o intuito de proteger uma comunicação, com a preocupação de que a mensagem, caso seja interceptada, não seja revelado o seu conteúdo. Desde o Império Romano, o imperador Júlio César utilizou um método que ficou conhecido como o Disco de César. Ele se comunicava com Cícero informando a ele suas táticas de guerra, dava comandos, entre outros assuntos que não deveriam ser revelados caso chegassem a pessoas que não fossem de sua confiança. Ele pensou em um alfabeto cíclico e substituía, por exemplo, a letra por uma terceira a sua direita podendo enviar suas mensagens sem se preocupar caso interceptassem o seu mensageiro:

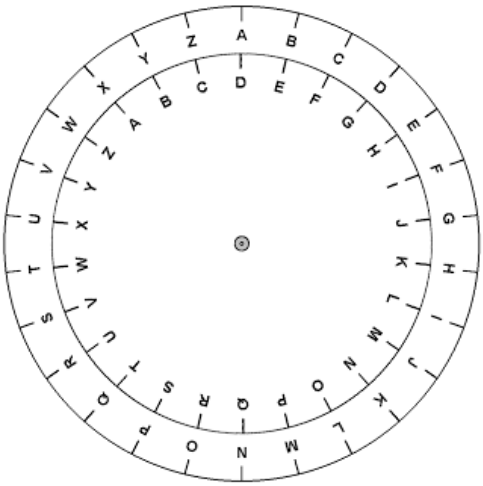


Figura 2.1 – Disco de César

Apenas Cícero e Júlio César sabiam qual era a “chave” para “descriptografar” a mensagem. Nesses casos, de criptografia por substituição, não costuma ser difícil o interceptor decifrar a mensagem criptografada, desde que ele disponha de tempo para analisar a mensagem e, por tentativa e erro, desvendar a chave. Para tanto, o interceptor pode observar a frequência relativa de caracteres na língua em que a mensagem foi escrita (ver figura 2.2) e compará-la com a que se encontra na mensagem criptografada, “quebrando” assim o segredo da mensagem. Por exemplo, 5 dos 44 caracteres da mensagem (2.2) correspondem à letra ´z´, e assim temos que a frequência relativa dessa

letra na mensagem é de (5/44) x 100 = 11%. Observando a figura 2.2, percebe-se que a frequência relativa das letras ´a´ ou ´e´ são superiores a 11%, o que traz a possibilidade

da letra ´z´ da mensagem criptografada representar a letra ´a´ ou a letra ´e´ (ou mesmo a letra ´o´ com menor probabilidade) na mensagem original. A substituição da letra ´z´ pela letra ´a´ resulta em:

nvhgi-**a**-wlm-**a**-xrlm-**a**-okilurhhrlm-**a**-ovnvmhrmlwvurhrx-**a** (2.3)

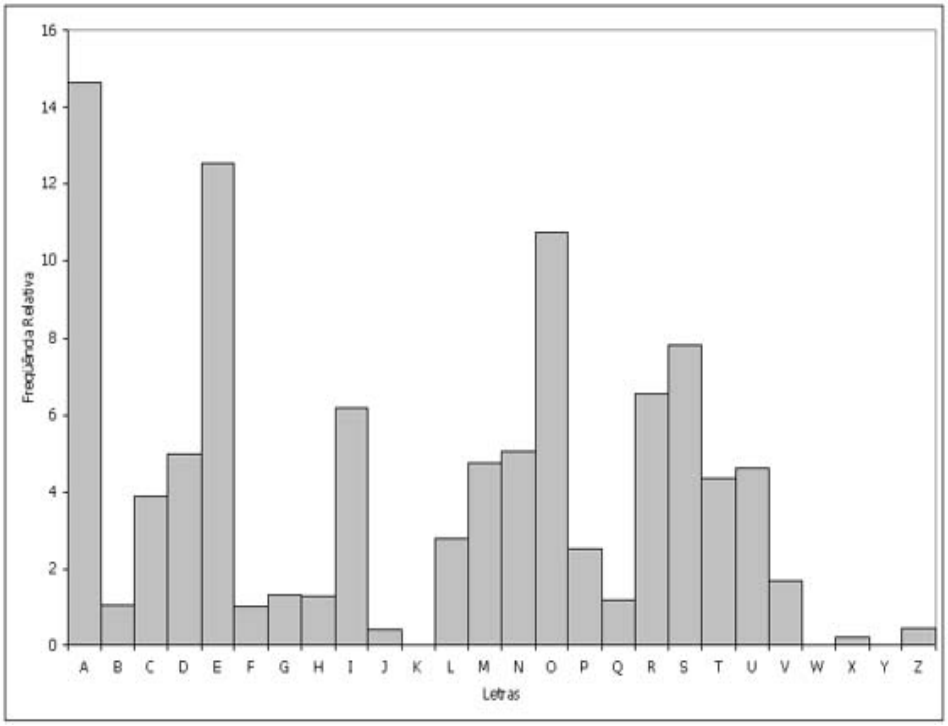


Figura 2.2 – Frequência relativa dos caracteres do alfabeto na língua Portuguesa. As quatro letras mais frequentes são a, e, o e s.

Ainda tentando decifrar a mensagem (2.2), temos que as frequências das letras *v* e *l* na mensagem criptografada são 9% e 11% respectivamente. Assim a letra *v* na mensagem criptografada poderia representar a letra *e* ou a letra *o*, na mensagem original. Já a letra *l* também poderia representar a letra *a* ou a letra *e* ou ainda a letra *o*. Como já utilizamos a letra *a* para substituir a letra *z*, iremos substituir *v* por *e* e o *l* por *o*. Isso resulta em:

n-**e**-hgi-**a**-w-**o**-m-**a**-xr-**o**-m-**a**-oki-**o**-urhhr-**o**-m-**a**-o-**e**-n-**e**-mhrm-**o**-w-**e**-urhrx-**a** (2.4)

Por tentativa e erro, construímos as correspondências até que se encontre uma mensagem que faça sentido e o código estaria decifrado. A mensagem acima corresponde à mensagem apresentada em (2.1), corroborando o método aqui apresentado para decifrar a encriptação.

2.2 - A chave aleatória

Métodos mais seguros são usados atualmente. Uma criptografia que não tenha uma correspondência unívoca entre o caractere da mensagem e o caractere que o encrípta será muito mais difícil de decifrar, senão impossível. Assim, não basta criar uma correspondência do tipo o caractere *a* vai no caractere *b* e o caractere *s* vai em *t* em toda a mensagem. É preciso que *a* seja transformado em *b* algumas vezes e em *f* outras vezes, por exemplo. A aleatoriedade é uma característica dos sistemas quânticos que é explorada na criação de uma chave aleatória como visto a seguir.

Os processos que fazem parte da comunicação criptografada moderna, entre o emissor e seu respectivo receptor, envolvem codificação e encriptação. A codificação representa a tradução dos caracteres de uma mensagem em uma sequencia binária de modo a permitir um tratamento computacional. Já a encriptação corresponde a uma operação lógica que transforma a mensagem codificada de forma que ela se torne ininteligível. No jargão da criptografia, a operação lógica é denominada “chave”, já que ela permite “fechar” e “abrir” a mensagem. Em geral, três etapas são necessárias para completar uma transmissão criptografada baseada no código binário.

Primeiramente, a mensagem deve ter seus caracteres codificados um a um em uma sequência de 0´s e 1´s (uma sequência binária ou sequência de bits). A correspondência entre os caracteres e as sequências binárias que os representam deve ser de amplo conhecimento de modo que o receptor consiga decodificar a mensagem. Para codificar uma mensagem escrita em nosso alfabeto, o qual contém 23 letras, é necessário pelo menos um conjunto de 5 bits, uma vez que $2^5 = 32$, o que é suficiente para representar as 23 letras. Se, no entanto, desejarmos incluir caracteres com a diferenciação entre letra maiúscula e minúscula, precisaremos de mais bits. A tabela 2.2 apresenta a codificação ASCII (American Standard Code for Information Interchange) dos caracteres do alfabeto que é usada nos computadores atualmente. Note que cada caractere é representado por uma sequência de 7 bits o que possibilita a codificação de

até 2^7 = 128 caracteres. Além das maiúsculas e minúsculas, existem caracteres extras, como números, sinais ortográficos etc, que necessitam de codificação.

Código Padrão Americano			
A	1000001	N	1001110
B	1000010	O	1001111
C	1000011	P	1010000
D	1000100	Q	1010001
E	1000101	R	1010010
F	1000110	S	1010011
G	1000111	T	1010100
H	1001000	U	1010101
I	1001001	V	1010110
J	1001010	W	1010111
K	1001011	X	1011000
L	1001100	Y	1011001
M	1001101	Z	1011010

Tabela 2.2 – Tabela de codificação ASCII traz o código que atribui valores numéricos aos caracteres como letras, números, sinais, etc.

Para diminuir a complexidade da etapa da codificação no produto proposto neste trabalho, usa-se como mensagem uma sequência genómica, já que este ´alfabeto´ biológico possui apenas 4 caracteres, os quais correspondem às iniciais das bases nitrogenadas presentes na estrutura do DNA: Adenina, Guanina, Timina e Citosina (A G T C, respectivamente). Assim precisaremos de apenas de 2 bits (pois 2^2 = 4) para representar cada uma das bases nitrogenadas do DNA (ver seção 2.3).

Em seguida, vem o processo da criptografia onde o emissor deve “misturar” sua mensagem com outra sequência de 0´s e 1´s, denominada chave. A chave deve ser conhecida apenas pelo emissor e pelo receptor e tem que ter um número de bits igual ao da mensagem que se deseja criptografar. Enfim, após a transmissão da mensagem criptografada, a última etapa é realizada pelo receptor que deve usar a chave para “descriptografar” a mensagem e então decodifica-la.

A Mecânica Quântica é útil em dois momentos do processo: na geração da chave e na sua transmissão. As propriedades quânticas dos fótons permitem saber se a transmissão da chave ocorreu de forma segura, ou seja, se o emissor e o receptor conseguem garantir que a chave é conhecida apenas pelos dois.

2.3 - Codificação e Encriptação de uma sequência genómica simples.

Pode-se criar uma correspondência entre uma sequência de caracteres e uma sequência binária. Tome-se como exemplo um pequeno trecho de um código genético:

T T A C T G G T A A (2.5)

Como as bases nitrogenadas que existem no DNA são 4, podemos codificar cada letra por uma sequência com 2 bits apenas. Poderia ser arbitrada a seguinte codificação:

A = 00
T = 01
G = 10
C = 11 (2.6)

Tabela 2.3 Código que atribui valores numéricos aos caracteres que formam a base nitrogenadas, semelhante ao código ASCII

Assim a mensagem representada pela sequencia na equação (2.5) seria codificada através de:

M = 01 01 00 11 01 10 10 01 00 00 , (2.7)

seguindo o sistema de codificação (2.6) acima.

Uma chave aleatória, como aquela mostrada abaixo, pode ser obtida por uma sequencia de sorteios:

CH = 00 11 00 00 10 10 10 01 11 10 (2.8)

Do ponto de vista quântico, uma chave como essa poderia ser gerada por uma sequência de medidas de um sistema quântico, como por exemplo, utilizar um sistema que emita um fóton por vez e medir sua polarização. Este sistema pode ser expresso por uma superposição entre dois estados: a polarização vertical e a polarização horizontal e um estado quântico não medido é descrito como uma função de onda que se expressa por uma superposição de estados:

$$|\psi\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \quad (2.9)$$

A medida provoca o colapso da função de onda, o que ocorre de maneira genuinamente aleatória (ver capítulo 3, seção 3.1). Assim, os resultados da medida da

polarização de um trem de fótons podem ser usados para exprimir uma sequencia binária aleatória. Para isso, bastaria associar a medida de uma polarização horizontal ao bit "0" e a medida de uma polarização vertical ao bit "1", ou vice-versa. Só para contrastar, no jogo de cara ou coroa é sempre possível, apesar de muito difícil, prever o resultado da jogada, pois a moeda segue o determinismo clássico, ou seja, dadas as condições iniciais do lançamento, a mecânica clássica define o que ocorrerá com a moeda a cada instante e dá uma previsão exata do resultado final. A medida não interfere no resultado. Ela apenas o revela. Na mecânica quântica, algo fundamentalmente diferente acontece. O resultado da medida é produzido por ela e não há um algoritmo, tal como as leis de Newton, que possa ser utilizado para prever o resultado da medida. O determinismo quântico é definido apenas para as probabilidades que o sistema deve obedecer, mas isso não garante nada sobre o resultado final de uma medida.

A encriptação da mensagem é obtida pela chamada operação lógica XOR, ou OU exclusivo, onde a mensagem em (2.7) é ´somada´ à chave (2.8) (ver tabelas 2.4 e 2.5 abaixo):

TABELA OPERAÇÃO LÓGICA XOR	0	1
0	0	1
1	1	0

Tabela 2.4 - Tabela operação lógica XOR: 0 XOR 0 = 0, 1 XOR 0=1,0 XOR 1=1, 1 XOR 1 =0.

M	0	1	0	1	0	0	1	1	0	1	1	0	1	0	0	1	0	0	0	0
CH	0	0	1	1	0	0	0	0	1	0	1	0	1	0	0	1	1	1	1	0
M XOR CH	0	1	1	0	0	0	1	1	1	1	0	0	0	0	0	0	1	1	1	0

Tabela 2.5 - Aplicação da operação lógica XOR na encriptação. Tem-se, na terceira linha, que m = M XOR CH

Nas tabelas acima, M é a mensagem original, m é a mensagem cirptografada e CH é a chave. É importante notar que a mensagem criptografada, quando decodificada é bastante diferente da mensagem original:

T G A C C A A A C G (2.10)

que pode ser comparada com a mensagem original:

T T A C T G G T A A (2.11)

Note que as três letras A na mensagem original (em 2.11) são transformadas em três letras distintas na mensagem criptografada (A, C e G respectivamente em 2.10), ou seja, existe a aleatoriedade desejada, a qual é introduzida pela chave.

Para recuperar a mensagem original, tem-se:

m XOR CH = M (2.12)

ou seja, aplicando-se novamente a chave na mensagem criptografada, a teremos a desencriptado, já que a dupla aplicação da operação lógica XOR resulta na identidade.

M	0	1	0	1	0	0	1	1	0	1	1	0	1	0	0	1	0	0	0	0
CH	0	0	1	1	0	0	0	0	1	0	1	0	1	0	0	1	1	1	1	0
M XOR CH	0	1	1	0	0	0	1	1	1	1	0	0	0	0	0	0	1	1	1	0
CH	0	0	1	1	0	0	0	0	1	0	1	0	1	0	0	1	1	1	1	0
M	0	1	0	1	0	0	1	1	0	1	1	0	1	0	0	1	0	0	0	0

Tabela 2.5 – Aplicando novamente a operação lógica XOR a Chave C. Tem-se que M = CH XOR m

CAPÍTULO 3

BASES CIENTÍFICAS DO PRODUTO

3.1 – Mecânica Quântica

A mecânica quântica é uma teoria construída para buscar o entendimento dos fenômenos microscópicos* e da luz. A interpretação dita ortodoxa desta teoria, na qual o entendimento dos fenômenos da natureza é intrinsecamente probabilístico, se baseia em sete postulados (COHEN-TANNOUDJI, C.1977). Dois desses postulados estão diretamente associados ao uso do produto proposto nesta dissertação. São eles: o princípio da *superposição dos auto-estados*, que corresponde à solução mais geral da equação de Schrödinger dependente do tempo, e o princípio do *colapso do vetor de estado*, que corresponde à influência de uma medida na evolução quântica de um sistema (M. A. V. Macedo. **2012**). Do ponto de vista matemático, a mecânica quântica é descrita em termos do problema de *auto-valores* e *auto-vetores* da álgebra linear. Tal qual um vetor no espaço bidimensional, que pode ser descrito em termos de uma *base* de vetores unitários ($\hat{x}$ e $\hat{y}$), o *vetor de estado* também admite decomposição em termos de uma *base* em um espaço vetorial: o chamado espaço de Hilbert. As probabilidades de ocorrência de um determinado fenômeno são definidas pelas componentes do *vetor de estado* em relação a uma determinada *base no espaço e Hilbert*.

Não se pretende aqui dar uma definição formal de todos os postulados que compõem a teoria quântica ou aprofundar sua descrição algébrica. Considera-se que uma descrição qualitativa seja suficiente para o entendimento das analogias entre os macrobits, que são os elementos principais do jogo proposto no produto, e os conteúdos da mecânica quântica enquanto disciplina formal. O apêndice 4 apresenta os postulados acompanhados de uma breve descrição de seus significados.

3.2 - Estabelecendo analogias

Tendo em vista o panorama pedagógico do trabalho, é importante formar

** O termo "microscópico" é um jargão da Física para denotar fenômenos na escala atômica e molecular.*

algumas analogias entre o conhecimento que os alunos detêm, como vetores no espaço bidimensional e a teoria de probabilidades, e o conteúdo que se deseja tratar de maneira que fiquem estabelecidas zonas de desenvolvimento proximal (Vygotsky apud MOREIRA A.M. em Teorias de aprendizagem, cap 7, 2014). As analogias aqui propostas visam ampliar a percepção dos alunos sobre o assunto. A visão científica da natureza requer a criação de uma entidade matemática para a descrição dos fenômenos. No caso da mecânica quântica, esta definição corresponde ao chamado *vetor de estado*, $|\psi\rangle^*$, o qual deve conter toda a informação possível sobre o sistema em estudo. O espaço vetorial usado para a descrição do *vetor de estado* pode ter dimensão infinita e se denomina espaço de Hilbert. Diferentemente da *base* do espaço bidimensional Euclideano ($\hat{x}$ e $\hat{y}$), a base do espaço de Hilbert é definida em termos dos chamados *auto-estados* $|\phi_n\rangle$ do problema** onde n é um número quântico que pode variar entre zero e infinito e está associado a um *auto-valor*.

Dentre os sistemas quânticos possíveis existem os chamados sistemas de dois níveis, os quais ficam bem definidos com apenas duas configurações. Neste caso, a base do espaço de Hilbert possui apenas dois *auto-estados* $|\phi_1\rangle$ e $|\phi_2\rangle$, sendo a analogia com o espaço $\mathbb{R}^2$ bastante ilustrativa. Em sua obra didática, Feynman dedica grande parte do volume III a estes tipos de sistema (R.P.Feynman**. Lições de Física.V3. Física Quântica**. 2018)

Uma moeda sobre uma mesa pode ser entendida como um exemplo macroscópico (meramente ilustrativo) de um sistema de dois níveis. Seguiremos este exemplo para ilustrar o funcionamento da aplicação da teoria. Os dois lados da moeda: "cara" ou "coroa", correspondem aos chamados *auto-estados* do sistema mencionados no primeiro parágrafo deste capítulo, e formam uma *base* para a descrição do *vetor de*

** Notação de Dirac: Ao contrário da Mecânica Clássica em que são usados vetores de até 3 dimensões no espaço Euclidiano, a notação de BraKet usada na Mecânica Quântica precisa de mais dimensões por ser um estudo probabilístico. Enfim, ela generaliza o conceito do vetor tridimensional.*

*** As informações sobre o estado do sistema físico na mecânica quântica, como posição, momento, spin etc,, é extraída pela aplicação dos chamados "operadores" ao vetor de estado. Estes correspondem a manipulações matemáticas sobre o vetor de estado (ver apêndice 4). Cada operador define um conjunto de auto-estados diferentes e os resultados das medidas correspondem aos chamados auto-valores do*

operador. A discussão dessa característica da teoria quântica é importante no aprofundamento de seu estudo. Do ponto de vista desta dissertação, tal discussão resultaria em um desvio demasiadamente grande do objetivo principal do trabalho.

estado. Com isso, o *vetor de estado* de uma "moeda quântica" é uma combinação linear (ou média ponderada, numa linguagem estatística) desses dois *auto-estados*, conforme a equação abaixo:

$$|\psi\rangle = c_1(t)|\phi_1\rangle + c_2(t)|\phi_2\rangle = \sum_{n=1}^{2} c_n|\phi_n\rangle \qquad (3.1)$$

onde $|\phi_1\rangle$ é um *auto-estado* que representa a face "cara" e $|\phi_2\rangle$ é um *auto-estado* que representa a face "coroa"*. A equação 3.1 corresponde àquilo que se denomina *superposição* de *auto-estados*. Os coeficientes $c_1(t)$ e $c_2(t)$ são determinados pela evolução dinâmica do sistema e como a soma das probabilidades dos possíveis resultados de medidas, de um determinado fenômeno deve ser unitária, teremos sempre que $|c_1|^2 + |c_2|^2 = 1$**

A equação (3.1) está de acordo com os postulados da mecânica quântica já que ela possui toda a informação sobre a "moeda quântica", no sentido de ser constituída por todas as configurações do sistema contendo os dois resultados possíveis de um jogo de cara ou coroa, por analogia. É importante mencionar que o *vetor de estado* mais geral possível descrito em (3.1) representa uma moeda que é simultaneamente "cara" e "coroa" o que, do ponto de vista clássico, é algo paradoxal (um disparate). No entanto, o que a mecânica quântica diz é que o *vetor de estado* governa apenas probabilidades. Assim, a interpretação da equação (3.1) é que, num instante t qualquer, a moeda tem probabilidade $|c_1(t)|^2$ de estar com a face "cara" para cima e $|c_2(t)|^2$ de estar com a face "coroa" para cima. A terminologia quântica moderna utiliza um termo específico para algo que esteja em um estado de superposição como o descrito pela equação (3.1): *q-bit*. A natureza "paradoxal" dos *q-bits* é a que se traduz no chamado paradoxo do

* Os auto-estados da "moeda quântica" $|\phi_1\rangle$ e $|\phi_2\rangle$ correspondem à vista superior da moeda quando ela é revelada. De certo modo, a operação de revelar a moeda é análoga a um operador posição na mecânica quântica.

**Interpretação estatística de Born, em que a probabilidade de encontrar uma partícula em uma dada posição é proporcional ao quadrado do módulo da função de onda, e a preditabilidade do formalismo se verifica somente para o comportamento médio das variáveis do sistema.

"gato de Schrödinger". Neste paradoxo, um *q-bit* é colocado juntamente com um gato dentro de uma caixa. O *q-bit* controla um sistema que libera um gás letal, e com isso o estado de superposição do *q-bit* é "transferido" para o gato que fica então em uma superposição de estados onde o animal está vivo e morto ao mesmo tempo. Dado que o resultado de uma medida não pode ser o estado de superposição, o sistema só pode ser encontrado em um de seus *auto-estados*, $|\phi_1\rangle$ ou $|\phi_2\rangle$, quando ocorre uma medição. Em termos de uma representação esquemática para o que ocorre com o *vetor de estado* no ato de uma medição tem-se:

$$|\psi\rangle = \sum_n c_n |\phi_n\rangle \xrightarrow{colapso} |\phi_m\rangle \tag{3.2}$$

Diz-se que o ato da medida colapsa o *vetor de estado* em um dos *auto-estados*. O estado de superposição anterior à medida fica então “dissolvido”, e a observação interrompe a evolução quântica do sistema trazendo-o para uma nova condição inicial. Isso se dá de forma completamente aleatória e indeterminada. É importante frisar que não há na teoria quântica nada que determine em qual dos *auto-estados* o *vetor de estado* irá colapsar no momento de uma medida. Mesmo que no instante imediatamente anterior ao da medida tivéssemos $|c_1(t)|^2 > |c_2(t)|^2 \neq 0$, o *auto-estado* $|\phi_2\rangle$ (o de menor probabilidade) pode ocorrer. Trata-se do evento mais genuinamente aleatório conhecido da Física. Esta característica da medida no âmbito da Física quântica é essencial na criptografia quântica, tal como descrito no capítulo anterior, pois é capaz de produzir uma sequência de resultados genuinamente aleatórios fornecendo a possibilidade de criação de uma chave perfeitamente aleatória indo de encontro do que foi dito na seção 2.2. Além disso, uma vez colapsado, o *vetor de estado* de uma partícula livre passa a ser conhecido e a repetição da medida dessa mesma propriedade retornará o mesmo resultado. Diz-se que o sistema encontra-se preparado, ou, que foi realizada a preparação do *vetor de estado*.

Os eventos mencionados acima podem ser descritos através de uma representação gráfica simples que está ao alcance de um aluno de ensino médio, conforme a figura 3.1, abaixo. Com isso, vale estabelecer uma zona de desenvolvimento proximal fazendo uma analogia de um sistema quântico de dois níveis com o caso dos vetores em duas dimensões, já que, para este caso, o espaço de Hilbert é bidimensional. A figura 3.1 ilustra um vetor juntamente com o círculo trigonométrico. Ao invés da base dos vetores unitários $\hat{x}$ e $\hat{y}$, do $\mathbb{R}^2$, temos a descrição do plano em termos da base dos *auto-estados* $|\phi_V\rangle$ ou $|\phi_H\rangle$ (V para vertical e H para horizontal). No espaço vetorial do plano cartesiano, o vetor representado na figura é descrito pela soma $\frac{\hat{x}+\hat{y}}{\sqrt{2}}$, enquanto o *vetor de estado* que descreve um tal *q-bit* é expresso por uma superposição de estados equiprováveis dado por:

$$|\psi\rangle = \frac{|\phi_V\rangle+|\phi_H\rangle}{\sqrt{2}} \tag{3.3}$$

Se o sistema possui evolução dinâmica, o *vetor de estado* evolui girando em torno da origem mantendo sua norma unitária como na parte esquerda da figura. No caso da medida ocorrer num instante em que o vetor de estado é aquele dado pela equação (3.3), ele colapsa com probabilidade de 50 % (já que $\{1/\sqrt{2}\}^2 = 0.5$) em um de seus *auto-estados* (como na parte direita da figura).

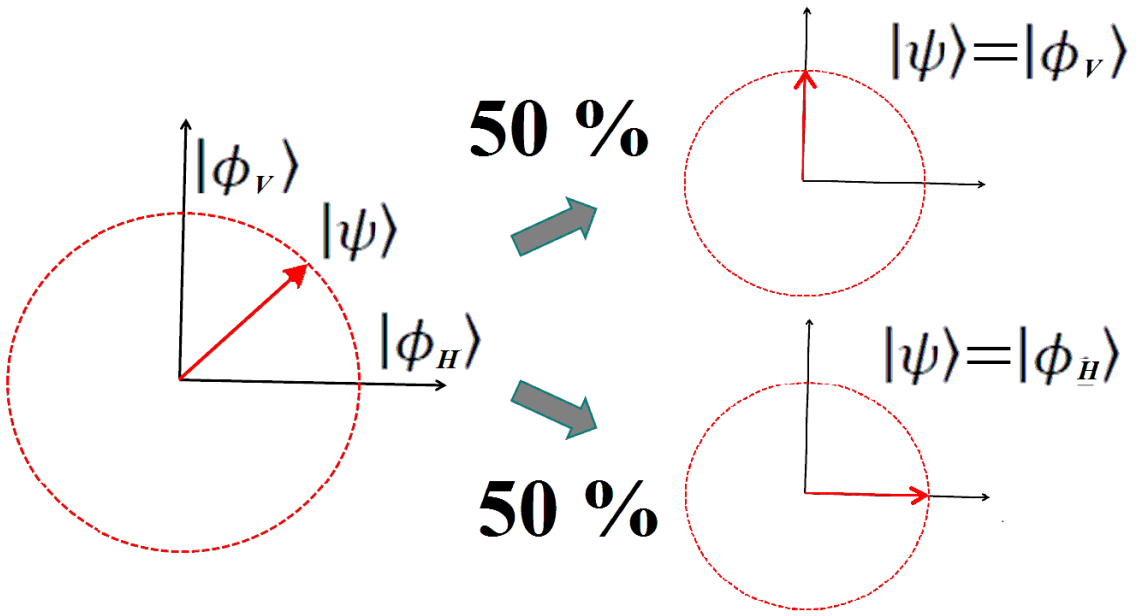


Figura 3.1 - Representação gráfica de um vetor de estado para um sistema de dois níveis. Um espaço vetorial (espaço de Hilbert) de duas dimensões fica definido em termos dos resultados possíveis para a medida.

Para o caso do sistema não ter evolução dinâmica (caso da partícula livre, por exemplo, onde os coeficientes c_1 e c_2 na 3.1 são constantes), o *vetor de estado* permanece em instantes posteriores no *auto-estado* que resultou do ato da medida inicial. A probabilidade de encontrar o sistema naquele determinado *auto-estado* em uma nova medida é igual à unidade, ou seja, o resultado de duas medidas iguais e consecutivas será certamente o mesmo.

É importante mencionar que as componentes do vetor de estado dependem da escolha da base. Assim, se uma base diferente for escolhida para a descrição do problema, o mesmo *vetor de estado* possuirá diferentes componentes em diferentes bases. Veja, por exemplo, a figura 3.2, que mostra a descrição de $|\psi\rangle$ (o mesmo da figura 3.1) em termos dos auto-estados $|\phi_A\rangle$ e $|\phi_D\rangle$ (A para Anti-diagonal e D para Diagonal), que estão inclinados em relação à $|\phi_V\rangle$ e $|\phi_H\rangle$. Na nova base, o *vetor de estado* $|\psi\rangle$ é escrito como $|\psi\rangle = 0\,|\phi_A\rangle + 1|\phi_D\rangle$, ou simplesmente

$$|\psi\rangle = |\phi_D\rangle \tag{3.4}$$

Assim, deve ser notado que, quando comparamos a (3.4) com a (3.3), vemos que os *auto-estados* de uma base são necessariamente descritos por uma superposição de estados em outra base. A base dos auto estados $|\phi_V\rangle$ e $|\phi_H\rangle$ é conhecida como base horizontal - vertical (VH). Já a base girada de 45^0, $|\phi_A\rangle$ e $|\phi_D\rangle$, é conhecida como base diagonal e anti-diagonal (DA).

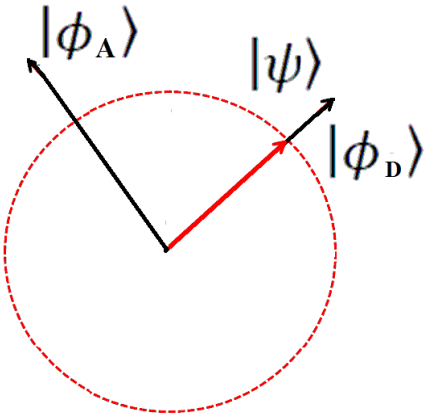


Figura 3.2 - Representação gráfica do vetor de estado da figura 3.1 após uma troca de base.

Curiosamente, e isso é uma característica da mecânica quântica, duas medidas consecutivas realizadas em bases diferentes retornarão resultados distintos mesmo no caso de uma partícula livre, onde não há evolução dinâmica do sistema. Se o *vetor de estado* $|\psi\rangle$ for medido na base (DA), como na figura 3.2, e logo a seguir for realizada uma nova medida, porém usando a base (VH), o resultado obtido pela segunda medida não é aquele representado pela equação (3.4). A previsão dada pela mecânica quântica é que, na nova medida, o *auto-estado* $|\phi_V\rangle$ terá 50% de chance de ocorrência e, correspondentemente, o auto-estado $|\phi_H\rangle$ terá a mesma chance de ocorrer, como na figura 3.1. Assim, o ato da medida no caso da mecânica quântica tem influência sobre o sistema (transformando $|\phi_D\rangle$ em $|\phi_H\rangle$, por exemplo). Como será visto, a mudança de base é uma das idéias centrais da criptografia quântica que é tratada nesse trabalho, e está relacionada à segurança da transmissão da chave criptográfica.

O exemplo da "moeda quântica" é ilustrativo, porém tem que ser ampliado para acomodar o entendimento do que significa uma mudança de base como aquela representada na figura 3.2. Essa ampliação é feita com um objeto que neste trabalho denominamos "macrobit": trata-se de um cilindro reto onde a base é pintada na cor preta, o topo é pintado na cor branca, metade da lateral é pintada de preto e a outra metade é pintada na cor branca (figura 3.3). Dessa forma, o macrobit tem quatro visualizações (projeções) possíveis quando observado ao longo dos eixos mostrados na figura 3.3.

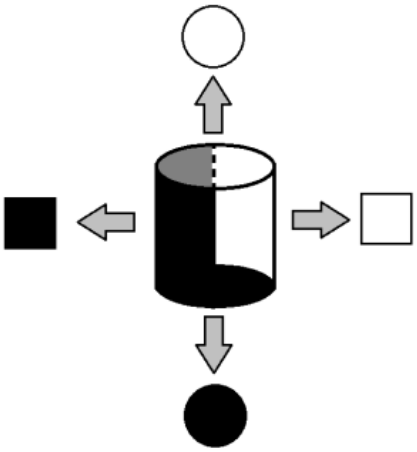


Figura 3.3 - O macrobit e suas quatro visualizações.

O *vetor de estado* do "macrobit" pode ser medido segundo dois critérios: forma ou cor. Pode-se dizer que cada um desses critérios corresponde a uma *base* sobre a qual o *vetor de estado* é projetado (em analogia à linguagem da mecânica quântica). Os critérios "cor" e "forma" para o "macrobit" são análogos às bases "VH" e "AD" para os *q-bits*. Temos então duas maneiras de escrever o *vetor de estado*, conforme as equações abaixo:

$$|\psi\rangle = c_1(t)|branco\rangle + c_2(t)|preto\rangle \tag{3.5}$$

$$|\psi\rangle = c_1(t)|quadrado\rangle + c_2(t)|bola\rangle \tag{3.6}$$

onde a equação (3.5) se refere à base "cor" e a equação (3.6) corresponde à base "forma". Dado o propósito de usar seguidas medidas de diversos macrobits para estabelecer uma chave aleatória, deve-se fazer uma correspondência do tipo binária ("0" e "1") para os resultados obtidos com os macrobits. Por exemplo, podem-se arbitrar as correspondências $|branco\rangle \rightarrow$ "0", $|preto\rangle \rightarrow$ "1", $|quadrado\rangle \rightarrow$ "0" e $|bola\rangle \rightarrow$ "1". Desse modo, e isso é importante para a segurança da criptografia, os resultados "1" e "0" podem ser obtidos de duas maneiras distintas. Vale fazer uma distinção entre o *q-bit* e o "macrobit", já que o último é um objeto clássico. Isso será feito na seção 4.2 onde detalhes da confecção e operação dos macrobits são descritos.

Como uma última observação, é importante mencionar que o "macrobit" está contextualizado na simulação do giro de um polarizador de um ângulo de 45^{o}. Assim a correspondência entre a mecânica quântica e a simulação do "macrobit" é que a base

vertical-horizontal é simulada pela "cor" da vista superior do "macrobit" e a base diagonal - antidiagonal é simulada pela "forma" da vista superior do "macrobit". Para ser mais específico, ainda que se possa dar uma conotação de que "forma" e "cor" representem diferentes operadores com auto-valores distintos (no caso quadrado e bola para o operador "forma" e preto e branco para o "operador" cor), isso não traria a interpretação desejada para este trabalho. No entanto, vale ressaltar que o "macrobit" pode, de fato, ser usado em outro contexto, para ilustrar a idéia de diferentes operadores atuando em um vetor de estado. Trata-se de outra aplicação para o conceito aqui apresentado.

3.3 - Realização física - o protocolo BB84

Um sistema quântico de dois níveis que está no contexto da criptografia quântica é o da polarização de fótons. Na teoria eletromagnética, a polarização corresponde à direção do campo elétrico da oscilação eletromagnética. Dado que o campo elétrico é um vetor no plano perpendicular à propagação da luz (ou do fóton no contexto da mecânica quântica), ele pode ser descrito em termos das componentes vertical e horizontal nesse plano, o qual é denominado de plano de polarização. Assim, do ponto de vista da mecânica quântica, a polarização do fóton pode ser descrita em termos de um *q-bit*. Nesse caso, o vetor de estado do fóton pode ser descrito usando-se a equação (3.1):

$$|\psi\rangle = c_1|\phi_1\rangle + c_2|\phi_2\rangle \tag{3.7}$$

Com isso, um fóton emitido por uma fonte luminosa, e que não tenha sofrido nenhum tipo de observação ou medida, está num estado de superposição do tipo gato de Schödinger como o da equação (3.7), onde foi adotado um fóton com polarização linear por simplicidade (nas polarizações circular e elíptica, os coeficientes c_1 e c_2 são funções do tempo).

Uma das maneiras de medir a polarização do fóton é se aproveitar do fenômeno da birrefringência, o qual se configura por uma anisotropia de certos materiais (o cristal de calcita é um exemplo), onde o índice de refração do material depende da polarização da luz incidente. Assim, a luz polarizada horizontalmente sofre um desvio diferente da luz polarizada verticalmente quando passa por um cristal de calcita, e isso resulta numa

separação espacial do feixe de luz incidente (figura 3.4). Com isso, podem-se usar dois detectores para registrar o resultado da passagem do fóton em um cristal de calcita, sendo um deles usado para detectar os fótons que colapsaram na polarização vertical (o detector "0" na figura 3.4), e o outro para detectar os fótons que colapsaram na polarização horizontal (o detector "1" na figura 3.4).

Neste ponto, vale mencionar que este é um mecanismo que torna possível a construção de uma sequência binária genuinamente aleatória que pode ser usada para compor uma chave criptográfica.

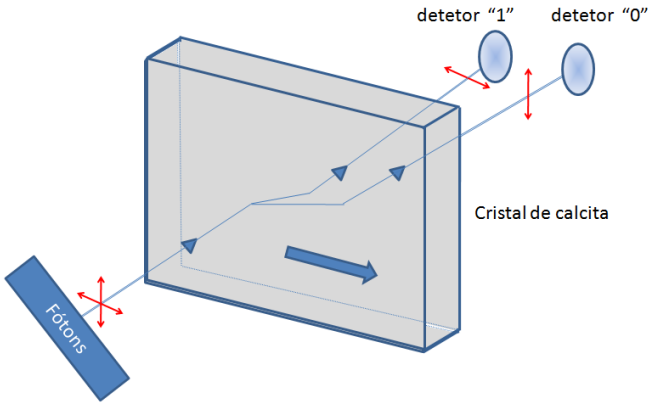


Figura 3.4 – Fenômeno de birrefringência que ocorre quando um fóton atravessa um cristal de calcita, polarizando a luz em direções diferentes de acordo com direção de escolha.

O que se tem a fazer é emitir certo número de fótons (gatos de Schrödinger) e fazê-los passar por um cristal de calcita, o qual promove uma bifurcação do caminho seguido pelos fótons. Dada a natureza aleatória do *vetor de estado* que descreve a polarização de cada fóton nesse trem de fótons, o acionamento dos detectores "0" e "1" ocorre ao acaso, e pode ser anotado como uma sequência de 0´s e 1´s genuinamente aleatória conforme a figura 3.4. Como visto a seguir, apesar de ser aleatória, esta sequência ainda não corresponde à chave criptográfica, pois a segurança da sua transmissão precisa ser também considerada. Outra etapa, mais engenhosa, usa um procedimento de "peneiração" para a construção da chave criptográfica no protocolo BB84 conforme visto a seguir.

A primeira etapa que os participantes de uma transmissão segura, o emissor e o receptor, devem cumprir é gerar, cada um deles, uma sequência aleatória por um conjunto de medidas como a que acaba de ser descrita. Ao final dessa etapa, tanto o

emissor quanto o receptor possuem sequências aleatórias distintas e independentes uma da outra. Estas sequências são usadas com objetivos distintos por cada participante do jogo.

Antes do início da produção da chave, os participantes devem combinar a correspondência entre as polarizações utilizadas e os valores binários, por exemplo, como na tabela 3.1. Esta correspondência pode ser de amplo conhecimento.

$\|\phi_V\rangle$	"1"
$\|\phi_H\rangle$	"0"
$\|\phi_A\rangle$	"1'
$\|\phi_D\rangle$	"0"

Tabela 3.1 - Correspondência entre auto-estados e valores binários.

O emissor usará sua sequência para fazer a preparação dos *vetores de estado* que descrevem os fótons que serão usados na transmissão criptográfica. Ele emprega sua sequência binária aleatória para definir qual base utilizará para transmitir cada fóton para o receptor. A mudança de base pode ser feita girando-se um polarizador linear de 45^o por exemplo (passando da base HV para a base AD). Deve ser notado que o emissor nada revela sobre o resultado das suas medidas. A tabela 3.2 ilustra o trabalho do emissor. Note que os bits que vão originar a chave estão entre aspas e obedecem a correspondência vista na tabela 3.1.

	Sequencia Sorteada pelo emissor	Base definida pelo sorteio	ket com a polarização do fóton	auto-valor ou "bit" enviado
1	1	VH	$\|\phi_V\rangle$	"1"
2	0	AD	$\|\phi_D\rangle$	"0"
3	0	AD	$\|\phi_A\rangle$	"1"
4	1	VH	$\|\phi_V\rangle$	"1"
5	1	VH	$\|\phi_V\rangle$	"1"
6	1	VH	$\|\phi_H\rangle$	"0"
7	0	AD	$\|\phi_A\rangle$	"1"

8	0	AD	$\|\phi_A\rangle$	"1"
9	1	VH	$\|\phi_H\rangle$	"0"
10	1	VH	$\|\phi_H\rangle$	"0"

Tabela 3.2 – A segundaa coluna traz uma sequência binária aleatória cujo valor está definido com a base AD e VH na terceira coluna, onde AD = 0 e VH = 1. A quarta coluna define a polarização do fotón que pode ser Vertical, Horizontal ou Antidiagonal e Diagonal. Conforme a polarização coincida com a base (consultar tabela 3.1) o bit enviado (quarta coluna da tabela) compõe a formação da chave.

Por sua vez, o receptor, usa sua sequência binária aleatória para selecionar a base que ele vai usar para medir os fótons enviados pelo emissor coletando os resultados. Também o receptor nada revela sobre o resultado das medidas realizadas. A tabela 3.3 ilustra o trabalho do receptor. Note que os bits que vão originar a chave estão entre aspas.

Segue-se uma etapa de conferência, no entanto, a conferência não se dá pelos valores dos bits ("0" ou "1") medidos por cada participante, mas sim pelo acordo entre as bases que cada um deles usou durante a transmissão. O receptor informa ao emissor qual base ele usou para e medição de cada fóton e o emissor, por sua vez, confirma se a base que ele usou para a preparação do fóton foi a mesma que o receptor usou. Note que o conhecimento da base nada diz sobre o valor que foi preparado pelo emissor e medido pelo receptor. O que fica garantido é que quando o emissor e o receptor usam a mesma base o resultado enviado pelo emissor é o mesmo que o receptor mede. Apesar do ordenamento das bases utilizado por cada participante ser diferente, existe a possibilidade de o emissor ter preparado um fóton de acordo com uma determinada base e, ao acaso, o receptor ter utilizado esta mesma base em sua medida, ou seja, o receptor mede o *auto-estado* produzido pelo emissor. Isso garante que a medida feita pelo receptor retorna o mesmo *auto-estado* que o emissor enviou (ver discussão sobre as figuras 3.1 e 3.2).

	Sequencia Sorteada pelo receptor	Base definida pelo sorteio	ket com a polarização do fóton	auto-valor ou "bit" recebido
1	0	AD	$\|\phi_V\rangle=\frac{1}{\sqrt{2}}(\|\phi_A\rangle+\|\phi_D\rangle)$	50% "1" + 50% "0"
2	0	AD	$\|\phi_D\rangle$	"0"
3	1	VH	$\|\phi_A\rangle=\frac{1}{\sqrt{2}}(\|\phi_V\rangle+\|\phi_H\rangle)$	50% "1" + 50% "0"

4	1	VH	$\|\phi_V\rangle$	"1"
5	0	AD	$\|\phi_V\rangle=\frac{1}{\sqrt{2}}(\|\phi_A\rangle+\|\phi_D\rangle)$	50% "1" + 50% "0"
6	1	VH	$\|\phi_H\rangle$	"0"
7	0	AD	$\|\phi_A\rangle$	"1"
8	1	VH	$\|\phi_A\rangle=\frac{1}{\sqrt{2}}(\|\phi_V\rangle+\|\phi_H\rangle)$	50% "1" + 50% "0"
9	1	VH	$\|\phi_H\rangle$	"0"
10	0	AD	$\|\phi_H\rangle=\frac{1}{\sqrt{2}}(\|\phi_A\rangle+\|\phi_D\rangle)$	50% "1" + 50% "0"

Tabela 3.3 – Na linha 1 temos uma superposição de estados na coluna ket, o que resulta numa probabilidade de 50/50 de termos um valor binário de 0 ou 1. Já na linha 2, como a base escolhida da terceira coluna coincide com a polarização do fóton, temos então um "0" como valor binário.

Essa coincidência ocorre cerca de 50% das vezes e somente os resultados onde ela existe são levados em consideração nesse processo chamado de "peneiração da chave". Os resultados onde as bases forem diferentes (os bits das linhas 1,3,5,8,10) são descartados pois não se pode garantir que a medida feita pelo receptor forneça o mesmo resultado que aquele enviado pelo emissor. Deve ser considerado que metade de uma sequência aleatória também é aleatória. A tabela 3.4 ilustra as possibilidades mencionadas acima e a chave criptográfica corresponde à sequência peneirada de acordo com o procedimento acima descrito.

Base Emissor	VH	AD	AD	VH	VH	VH	AD	AD	VH	VH
Base receptor	AD	AD	VH	VH	AD	VH	AD	VH	VH	AD
Bit da chave peneirada	x	"0"	x	"1"	x	"0"	"1"	x	x	"0"

Tabela 3.4 – A base emissor quando coincide com a base receptor fornece um bit que será usado para a construção da chave.

Assim, a chave corresponderia à sequencia 01010. O procedimento acima descrito deve ser repetido até que se tenha uma chave com um número de bits grande o suficiente para encriptar uma mensagem.

A segurança da chave ocorre, pois qualquer leitura da sequencia de fótons enviada pelo emissor introduz 50 % de erro nos resultados, ou seja, aproximadamente metade dos resultados deve ser descartada no processo. Assim, se um interceptor medir os fótons enviados pelo emissor e retransmiti-los para o receptor, a contagem de erros será de 75% entre o receptor e o emissor o que denuncia a ação do interceptor.

CAPÍTULO 4

CONFECÇÃO DO PRODUTO

4.1 – Introdução

A criação do jogo dos Macrobits foi um processo que levou certo tempo para ser concluído uma vez que trazer para o mundo macro algo que acontece na escala do mundo micro, como é o caso dos sistemas governados pela Mecânica Quântica, a princípio pode parecer impossível. E na verdade é, porém a ideia do comportamento das partículas, do funcionamento dos fenômenos e de suas características mais importantes que podem ser traduzidas de forma que seja possível entendermos seus significados e desenvolver uma maneira de pensar que envolva os conceitos da Mecânica Quântica. Um exercício de imaginação tornou possível criar as regras do jogo, suas peças, acessórios e tabelas que “concretizam” as ideias da Mecânica Quântica no produto.

4.2 - Os Macrobits

Os Macrobits são as peças de maior importância do Produto, pois conforme a discussão na seção 3.2, são eles que caracterizam no jogo o significado dos q-bits. Tal qual um "gato de schrödinger", um "macrobit" dentro de uma caixa fechada pode ser pensado como estando em um estado de superposição. Antes de se realizar uma medida, ou seja, antes de abrir a caixa, tudo o que se pode dizer é que existe um "macrobit" no interior da caixa descrito por um vetor de estado $|\psi\rangle$. Antes de realizar a medida, um observador deve selecionar um critério para determinar qual resultado deve ser coletado. Nos termos técnicos da mecânica quântica, diz-se que a base na qual o vetor de estado será projetado deve ser definida pelo observador antes da realização da medida. O estabelecimento da base corresponde, no jogo, à escolha do critério (forma ou cor) que será usado para escrever o resultado no momento da abertura da caixa e revelado seu conteúdo (no caso o resultado corresponde à identificação da vista superior do macrobit quando a caixa é aberta). A figura 4.1 abaixo ilustra a situação acima descrita. (a) O macrobit mostrado na figura pode ser coberto pelo recipiente opaco de modo a simular a situação onde existe um *q-bit* no interior de uma caixa. (b) Uma vez coberto, o macrobit

fica em um estado indeterminado análogo (porém conceitualmente diferente) à superposição de estados do gato de Schrödinger. (c) A retirada do copo (ato da medição) revelará qual das quatro possíveis projeções (vistas superiores) será o resultado da medida.

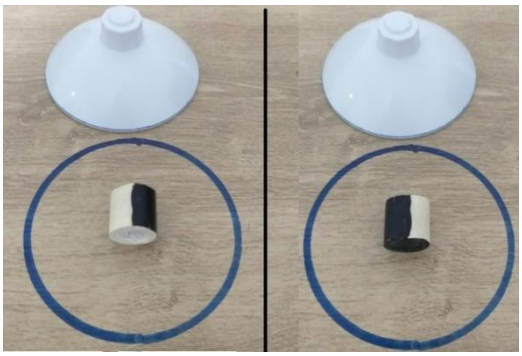


Figura 4.1 - (a) Representação de um q-bit que pode estar dentro da caixa

Figura 4.1 - (b) Simulação da superposição de estados

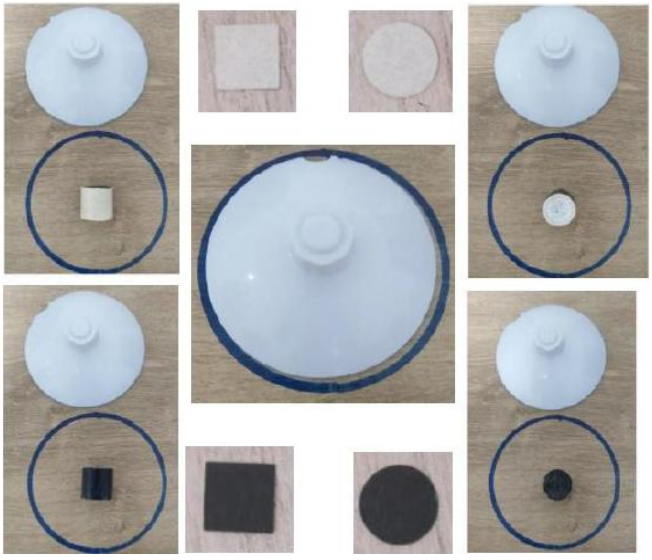


Figura 4.1 - (c) Simulação dos possíveis resultados da medida

Cabe aqui ressaltar a diferença entre o *q-bit* e o macrobit já que o último é um objeto clássico. Se elegermos o critério "cor" para a medida do "vetor de estado" de um macrobit, os resultados que serão anotados pelo observador serão aqueles que correspondem aos *auto-estados* $|branco\rangle \rightarrow$ "0" ou $|preto\rangle \rightarrow$ "1". Apesar disso, no momento da medida do macrobit, a sua "forma" está visível e poderia ser computada, ou seja, não há colapso do *vetor de estado* uma vez que a propriedade "forma" não se torna indisponível para uma medida no caso clássico. Isso já não acontece no caso do *q-bit*, pois se a medida for feita de acordo com uma determinada base, a leitura do vetor de estado na outra base fica impossibilitada no sentido de que o *auto-estado* resultante após a medida é, necessariamente, uma superposição de estados em outra base (como visto na discussão das figuras 3.1 e 3.2). Assim, cada característica só "existirá" independentemente da outra de acordo com a *base* pré-selecionada pelo jogador, seja ele o emissor ou o receptor. O fato do Macrobit ter sua característica definida pelo critério escolhido pelo jogador é o que traduz o fenômeno do colapso do *vetor de estado* no âmbito do jogo, ou seja, só teremos certeza do tipo de Macrobit que está no jogo quando o medirmos e obtermos sua informação (forma ou cor) definida pelos critérios usados pelos jogadores.

4.3 - A confecção do jogo

As peças que compõem o jogo foram adaptadas das ideias apresentadas nas seções anteriores. O cilindro representando o macrobit da figura 3.3 foi produzido apenas com o propósito de ilustrar o mecanismo do jogo. Por comodidade e facilidade operacional, as peças manipuladas pelos alunos consistem nas 4 projeções mostradas na figura 4.2. Tais projeções foram confeccionadas utilizando uma cartolina com faces de cores diferentes, um lado preto e outro branco, e essa cartolina foi recortada em dois tipos de formato; bola (círculo) e quadrado. Os cortadores foram adquiridos em uma casa de produtos para festa e a cartolina em uma papelaria (a um custo inferior a R$50,00).

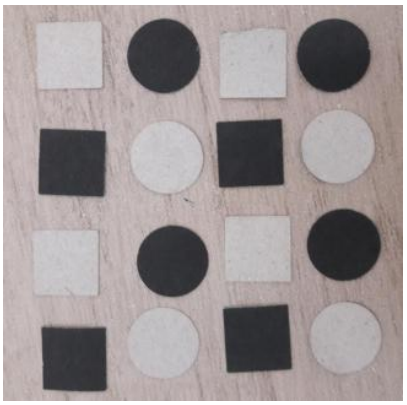


Figura 4.2 – ***Macrobits feitos de cartolina***

Figura 4.3 – ***Cortador de cartolina no formato de bola***

Figura 4.4 – Cartolina de duas faces (preto e branco)

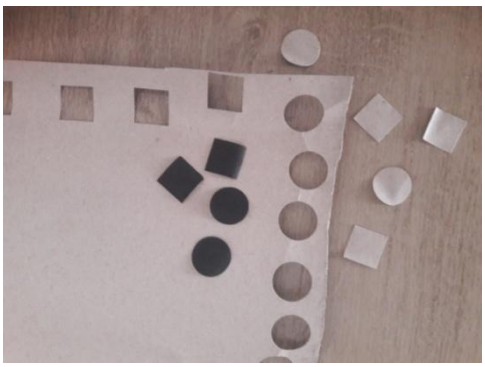


Figura 4.5- Face branca da cartolina e macrobits com as duas faces e duas formas

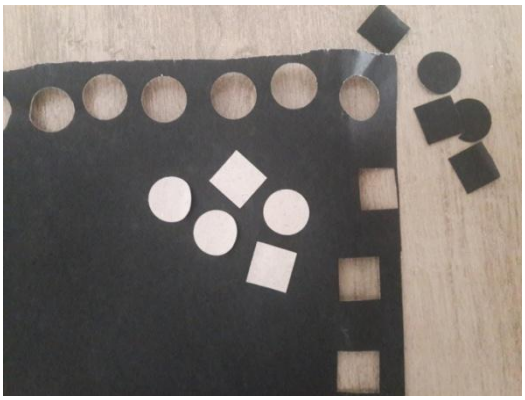


Figura 4.6 – Cartolina com a face preta e macrobits com as duas faces e duas formas

A régua é um suporte para posicionar as projeções dos Macrobits na ordem que são selecionadas; esta ordem é sorteada aleatoriamente, sendo as peças retiradas de uma urna, uma a uma. A sequência do sorteio das peças deve ser respeitada, assim como a face voltada para o jogador (face branca ou face preta). A régua possui uma indicação da ordem de sorteio dos Macrobits para que os jogadores possam seguir esta sequência, assim coletam os dados de cada peça para a criação da Chave em um momento mais adiante do jogo.

O sorteio dos Macrobits para posiciona-los na régua suporte tem a função de reproduzir a ideia de aleatoriedade dos fótons emitidos como na figura 3.4, como as peças são sorteadas de uma urna e cada peça possui duas características que podem ser analisadas, isso nos dá a ideia de não sabermos qual é a informação enviada até o momento em que seja analisada a peça de acordo com as bases dos jogadores.

A régua suporte é simplesmente uma canaleta de encadernação transparente, onde desenhamos com caneta permanente uma seta que indica a ordem que os Macrobits foram sorteados, e a numeração de cada peça posicionada. Assim facilita a leitura de cada Macrobit dificultando a contagem errada das peças quando as prendemos nesta canaleta como uma folha de papel comum. Essa mesma peça do jogo é usada tanto pelo emissor quanto pelo receptor. O fato da canaleta ser transparente é de suma importância para que os jogadores possam ver a face do Macrobit que está voltada para frente, para caracterizar a sua cor. Lembrando que tanto o formato da

peça como sua cor são informações que devem ser extraídas para a construção da Chave, que é o objetivo do jogo.

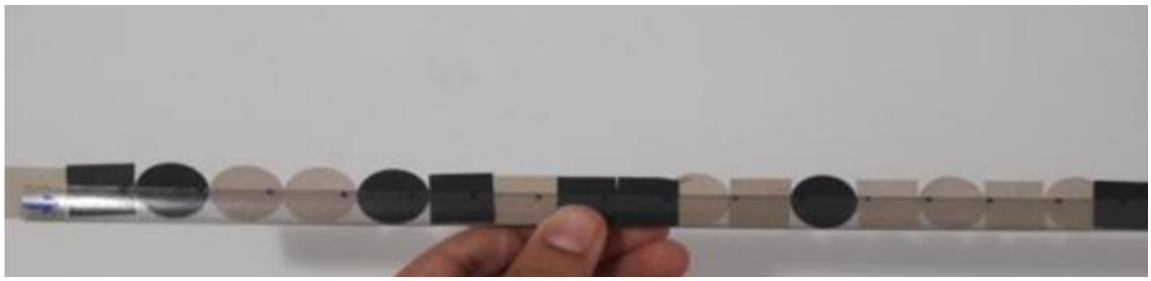


Figura 4.7 – Régua suporte de macrobits

Para que se possa construir a Chave que irá criptografar a mensagem secreta do jogo é necessário que cada jogador (emissor e receptor) construa a sua Base de forma aleatória. A Base é composta por uma sequência de características que devem ser extraídas dos Macrobits que estão na Régua Suporte, essas características são a forma ou a cor da peça. Os dados são usados justamente para que as características da Base a ser construída sejam de acordo com os números que os dados forneçam ao serem jogados pelo emissor e receptor. Números impares equivalem a cor do Macrobit e números pares, a forma:

Impar	Par
1 - 3 - 5	2 – 4 - 6
Cor	Forma

Figura 4.8 – tabela forma-cor: essa tabela codifica os números sorteados no dado nas duas opções de base para o macrobit.

O uso dos dados também tem a finalidade de dar a ideia de aleatoriedade para a construção da sequencia das bases (conforme as tabelas 3.2 e 3.3), mais uma vez reproduzindo uma importante característica da Mecânica Quântica.

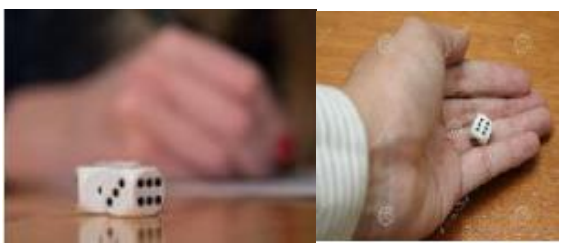


Figura *4.9 – dados usados pelo emissor e receptor para escolher a base*

Os Dados usados são os mesmos usados em jogos de tabuleiro, com 6 faces enumeradas de 1 a 6, onde os números impares correspondem à Cor do Macrobit e os números impares correspondem à Forma do Macrobit.

As tabelas (apêndice 1) são como duas cartelas que têm a função de organizar todas as informações que estão no jogo, ou seja, a Base, os Macrobits, a Chave e a Mensagem. São duas Tabelas divididas em 5 colunas; Base,Macrobits, Informação, Checagem e Chave. Na cartela também existem 5 quadros; um quadro da Tabela Porta XOR, outro de codificação da mensagem, o quadro que relaciona os números dos dados a informação que constituirá a Base, uma tabela que tem a função de legenda que associa a característica do Macrobit com a informação que ele fornece e um quadro onde o jogador faz a Soma de Base 2.

São duas Cartelas, uma para o Emissor (apêndice 1.1) e outra para o Receptor (apêndice 1.2), onde os jogadores irão completar as colunas simultaneamente sendo orientado pelo professor. Ao final será formada a Chave, e com ela o Emissor criptografa a mensagem e o Receptor "descriptografa" e confere a mensagem. A diferença entre as duas tabelas (tabela do Emissor e a tabela do Receptor) está apenas no quadro onde se faz a aplicação da porta XOR para criptografar a mensagem secreta (no caso do Emissor) e descriptografar a mensagem (que é o caso do Receptor).

Chave				
Mensagem				
Mens.Criptografada				

Figura 4.10 – tabela de encriptação da mensagem usada pelo emissor

Chave				
Mens.Criptografada				
Mensagem				

Figura 4.11 – tabela de desencriptação da mensagem usada pelo receptor

A tabela deve ser bem organizada, com um "layout clean" para que os jogadores não se percam durante o processo e o jogo possa ocorrer sem imprevistos e erro. Qualquer falha ao preencher a tabela inviabiliza o objetivo final do jogo, pois as sequências devem ser respeitadas e cada informação é imprescindível para a criação correta da Chave.

CAPÍTULO 5

APLICANDO O PRODUTO

5.1 – Introdução

Este capítulo relata como o produto foi aplicado em uma sala de aula aos alunos do ensino médio, suas reações ao serem apresentados ao jogo, como foi conduzido o jogo, a apresentação das etapas e como isso os ajudou a abordar a mecânica quântica em sala de aula.

Antes do produto ser aplicado em sala de aula com os alunos do ensino médio, ele foi testado via skype com uma que reside no estado de Minas Gerais. Essa pessoa não possui formação na área cientifica nem na de ensino, ou seja, uma pessoa leiga no assunto. O fato dos jogadores estarem em ambientes bem distintos, um em Minas Gerais e o outro no Rio de Janeiro e se comunicando apenas pela webcam, deu mais credibilidade ao funcionamento do jogo em relação a transmissão de uma mensagem secreta entre duas pessoas. O receptor não teria como acessar a mensagem a não ser se participasse do jogo.

Foram explicadas as regras do produto conforme o jogo ia se desenvolvendo, o emissor ia passando os comandos ao receptor do que ele teria que fazer: sortear a base, anotar a informação dos macrobits, etc. Ao final, quando a chave foi criada e o receptor conseguiu traduzir a mensagem, ficou claro o funcionamento do jogo e que era possível aplica-lo não só em sala de aula mas também numa situação a longa distância.

Foi escolhido um colégio da rede privada de ensino, da zona norte do Rio de Janeiro, onde o professor se sentia mais a vontade de aplicar o produto em função da liberdade que a coordenação da instituição dava aos professores. As turmas escolhidas tinham um número razoável de alunos, por volta de 22 alunos cada, o que também contribuiu para a aplicação do produto devido a facilidade de poder dar assistência a cada aluno que participara da atividade. Os alunos variavam sua faixa etária entre 15 e 17 anos, número bem equilibrado de meninos e meninas, que na sua maioria pertenciam a uma classe média. Cada turma tinha em média de 2 alunos que eram bolsista, mas o

que praticamente predominava em ambas as turmas era a quantidade de alunos que na sua maioria estudava nessa instituição desde as séries iniciais. Um detalhe que vale a pena comentar era o número muito baixo de alunos que tinham pretensão de seguir a carreira na área das ciências ou qualquer área relacionada a Física.

A primeira vez que esta atividade foi aplicada foi para uma turma de 3° série do ensino médio, e no mesmo dia para uma turma de 2° série também do ensino médio. Isso foi feito em dois tempos de aulas consecutivos, um tempo para cada turma, o que pareceu suficiente desde que o professor esteja bem familiarizado com o produto e saiba aplica-lo com objetividade.

5.2 - O convite

O professor chegou para mais um dia de aula, como esperavam os alunos, porém os surpreendeu perguntando-lhes se gostariam de participar de um jogo. A reação imediata dos alunos foi perguntarem que jogo seria esse, mesmo quase já aceitando de imediato. O professor respondeu que seria um jogo de "adivinhação" que lhes daria conhecimentos de física, mais especificamente sobre Mecânica Quântica. As reações foram diversas: desde empolgação, curiosidade, até desconfiança, medo e desânimo. Mas, mesmo assim, aceitaram entrar no jogo e com isso vieram dúvidas sobre qual seria a dificuldade de se jogar, se era necessário saber física, se iriam se sentir constrangidos e etc. Então foi esclarecido que o objetivo do jogo era criptografar uma mensagem tornando-a secreta, e a enviando sem que ninguém conseguisse decifra-la, exceto o seu destinatário. Que usaríamos métodos que se assemelham aos fenômenos da mecânica quântica para pode dar mais segurança na transmissão da mensagem secreta. Após esses esclarecimentos e o "sim" dado pelos alunos, a turma foi dividida em dois grupos, um deles o grupo emissor e o outro grupo o receptor.

5.3 - A apresentação

Aos alunos foram apresentadas as regras e ideias gerais do jogo; que se tratava de um grupo escrever uma mensagem e criptografa-la, ou seja, fazer desta mensagem uma mensagem secreta e enviar ao outro grupo. O outro grupo por sua vez teria uma forma de "quebrar" esse segredo e descobrir qual o conteúdo da mensagem. Para isso era necessário criar a chave, ou seja, utilizando os Macrobits se constrói uma sequência de dados que é a "chave" para encriptar e desencriptar a mensagem transmitida.

Algumas informações e esclarecimentos foram necessários para que pudessem entender o jogo e assim participar, como o que é código Binário, Tabela operação lógica XOR, tabela ASCII e outros termos que fazem parte da linguagem usual da criptografia. Já a linguagem usual da mecânica quântica não foi utilizada no momento do jogo, pois a ideia do jogo era justamente fazer com que os alunos desenvolvessem conhecimentos prévios, adquirissem essa linguagem de maneira indireta e que isso os ajudasse no aprendizado da mecânica quântica.

O código binário era de conhecimento da maioria dos alunos, mas não todos, que tinham noção que essa linguagem fazia parte do mundo digital, e que era representado por zeros “0” e uns “1”. A codificação, ato de traduzir para o código binário caracteres do nosso alfabeto, por exemplo, foi algo que ao ser apresentado a eles trouxe bastante surpresa e curiosidade da maioria. Mesmo alguns alunos que já tinham noção do que era o código binário se surpreenderam com essa aplicação de codificar uma mensagem ou informação. Essas informações tiveram que ser dadas aos alunos, pois eles precisavam codificar a mensagem que será criptografada, a mensagem era uma sequência genómica (A T C G) criada por eles mesmos e/ou pelo professor. E essa mensagem codificada precisa ser somada a chave criptográfica através da operação lógica XOR.

A tabela operação lógica XOR foi algo que eles nunca tinham visto ou ouvido falar, por isso foi necessário uma demonstração no quadro negro para que todos pudessem aprender e entender o que fazer com ela. Durante o jogo, a tabela ficou exposta no quadro durante todo o tempo para que pudessem consulta-la. A tabela tem a função de criptografar a mensagem utilizando a chave, fazendo a aplicação da operação lógica XOR (0+0=0, 0+1=1, 1+1=0, 1+0=1). Até então, essas informações foram extremamente necessárias para que eles pudessem jogar, sem esses conhecimentos os alunos não conseguiriam desenvolver nenhuma capacidade de conexão do jogo com a mecânica quântica.

5.4 - As regras

Após essas primeiras informações ensinadas aos alunos o segundo momento foi apresentar as regras do jogo.

As tabelas foram distribuídas aos dois grupos, emissor e receptor, lembrando que as tabelas são diferentes no quadro em que se adiciona a mensagem criptografada, a chave criptográfica e onde se desencripta a mensagem. Na tabela do emissor a sequência é MENSAGEM – CHAVE – MENSAGEM CRIPTOGRAFADA, já na tabela do receptor a sequência é MENSAGEM CRIPTOGRAFADA– CHAVE – MENSAGEM.

Nas cartelas, temos várias informações a serem preenchidas, e a que requer maior atenção é a tabela onde se constrói a base, onde se peneira os macrobits e se forma a chave criptográfica.

A primeira coluna é onde os grupos formam suas bases em uma sequência totalmente aleatória jogando seus dados. Sorteando números ímpares, a FORMA do Macrobit deve ser a base característica: caso sejam sorteados os números pares, seria a COR do Macrobit a base característica. Aqui temos a representação do VETOR DE ESTADO na mecânica quântica, como está indicando na figura 3.3 e representado nas equações 3.5 e 3.6.

Tanto o emissor quanto o receptor devem construir suas bases usando os dados, cada grupo fez isso sem que o outro grupo visse ou tivesse acesso às informações, conforme a discussão das tabelas 3.2 e 3.3. Após o sorteio da base, o professor fez o sorteio, também aleatório, da sequência de macrobits que foram expostos na régua para serem apresentados aos grupos. O sorteio desses macrobits foi feito de maneira que todos vissem que as peças estavam sendo retiradas de uma urna e colocadas em sequência na régua. Aqui também foi enfatizado que os macrobits estavam sendo sorteados aleatoriamente, como no sorteio dos números do jogo de bingo, por exemplo. Porém, a face do macrobit também é importante, uma vez que temos uma face da cor branca e a outra da cor preta, e a diferença das cores nas faces é o que representa o AUTO ESTADO DA FUNÇÃO DE ONDA, como abordado na seção 3.2.

5.5 - Retirando as informações dos macrobits

Quando o professor ia sorteando os macrobits, os alunos retiravam as informações do mesmo segundo suas bases sorteadas anteriormente. Caso a base fosse COR era retirada a informação cuja cor estava voltada para ele na régua, BRANCO OU

PRETO; caso fosse FORMA, a informação retirada poderia ser BOLA ou QUADRADO como indicava aquele macrobit.

Neste momento, nenhum dos grupos deve cometer erro ao retirar a informação segundo sua base. Por isso, o professor sempre os alertava do cuidado nessa fase do jogo, pois um erro na sequência prejudica todo o jogo sendo necessário recomeçar tudo novamente. E ao final dessa etapa, mostrou-se aos grupos que a informação que cada um terá é completamente aleatória e com probabilidade de apenas 50% da informação coincidir com do outro grupo conforme apresentado na seção 3.3 e na discussão da tabela 3.4.

Essas informações que foram retiradas é que formaram a chave quântica para criptografar a mensagem, mas para isso é necessário fazer a checagem ou "peneira" dos macrobits. Outro momento em que também não podem ocorrer erros por parte dos jogadores. Aqui o grupo receptor começou a "cantar" para o grupo emissor qual era a sequência da sua base. Quando as bases coincidiam a informação extraída daquele Macrobit era usada na construção da chave para ambos os grupos, caso a base fosse diferente se descartava a respectiva informação do Macrobit. Assim, ao final da peneira, os dois grupos tinham uma chave quântica, que para o grupo emissor teve a função de criptografar a mensagem codificada, e, para o grupo receptor, descriptografar.

5.6 - Quebrando o segredo

Após a peneira, a chave criptográfica estava pronta, a mensagem então foi criptografada pelo emissor e entregue ao receptor. O receptor por sua vez desencriptou a mensagem usando a tabela operação lógica XOR e obteve uma mensagem codificada. Descodificando a mensagem, foi revelada a mensagem original que continha uma sequência de quatro dígitos da cadeia genómica, coincidindo exatamente com a mensagem criada pelo grupo emissor. Daqui em diante, a curiosidade e as dúvidas começaram a tomar conta dos alunos, cada um com sua teoria, tentativas de desvendar o "mistério" e muitas perguntas. Como era possível? Como a física fazia isso acontecer? Qual era o truque?

Após a aplicação do jogo, o professor abriu para debate questões como: já tinham ouvido falar da mecânica quântica? o que eles sabiam a respeito? como tiveram acesso a esse tema? Ouviram falar do gato de Schrödinger?

O professor percebeu que o jogo deu maior tranquilidade para abordar esse tema, a aplicação do jogo serviu como exemplo concreto para representar os fenômenos quânticos e dar um acesso mais fácil aos alunos. Notou-se que as ideias do mundo micro, como é na mecânica quântica, foram bem representadas na escala macro, apesar da complexidade e estranheza desses fenômenos. Claro que muitas dúvidas ainda permeavam os alunos, mas o jogo teve um resultado positivo em trazer para a sala de aula o debate sobre esse tema. E mais, deu aos alunos ferramentas para que pudessem discutir e interagir com a mecânica quântica.

A outra turma que também participou do jogo teve reações similares à primeira. E abaixo temos duas figuras que mostram as tabelas preenchidas durante uma simulação do jogo, onde a primeira cartela é a do Emissor, que fica encarregado de criptografar a mensagem e transmiti-la ao Receptor. A outra cartela é do Receptor, que também cria a chave aleatória com o objetivo de revelar o segredo da mensagem criptografada.

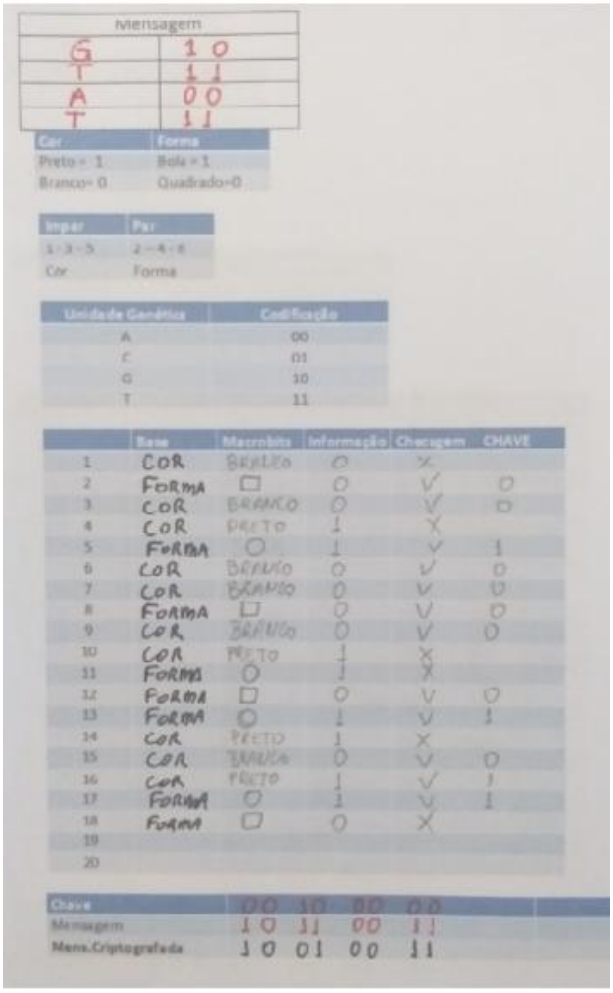
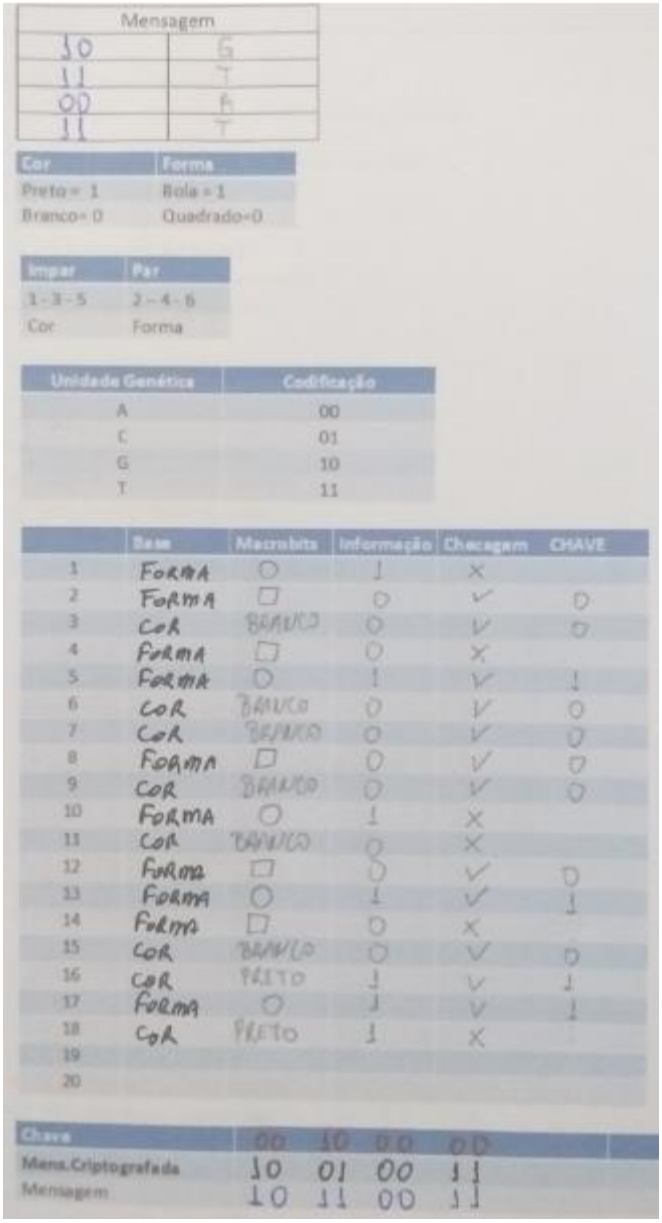


Figura 5.1 – Cartela do Emissor

Temos a primeira coluna da tabela onde foram criadas aleatoriamente as sequências das bases que constituem de forma ou cor. Já a última coluna é a chave criada também de forma aleatória que criptografa a mensagem do emissor e descritografa a mensagem do receptor.



Mensagem	
10	G
11	T
00	A
11	T

Cor	Forma
Preto = 1	Bola = 1
Branco= 0	Quadrado=0

Impar	Par
1 - 3 - 5	2 - 4 - 6
Cor	Forma

Unidade Genética	Codificação
A	00
C	01
G	10
T	11

	Base	Macrobits	Informação	Checagem	CHAVE
1	FORMA	○	1	X	
2	FORMA	□	0	✓	0
3	COR	BRANCO	0	✓	0
4	FORMA	□	0	X	
5	FORMA	○	1	✓	1
6	COR	BRANCO	0	✓	0
7	COR	BRANCO	0	✓	0
8	FORMA	□	0	✓	0
9	COR	BRANCO	0	✓	0
10	FORMA	○	1	X	
11	COR	BRANCO	0	X	
12	FORMA	□	0	✓	0
13	FORMA	○	1	✓	1
14	FORMA	□	0	X	
15	COR	BRANCO	0	✓	0
16	COR	PRETO	1	✓	1
17	FORMA	○	1	✓	1
18	COR	PRETO	1	X	
19					
20					

Chave	00	10	00	00
Mens.Criptografada	10	01	00	11
Mensagem	10	11	00	11

Figura 5.2 – Cartela do Receptor

CAPÍTULO 6

Resultados

6.1 - Introdução

Meses após a aplicação do jogo, e de toda a discussão em sala de aula sobre a Mecânica Quântica no ano anterior, foi dado aos alunos um questionário para que eles pudessem responder sobre o tema Física Quântica. O grupo de alunos do ensino médio é o mesmo do colégio em que foi aplicado o produto. O questionário com respostas objetivas de múltipla escolha (*apêndice-2.1*) tinha o intuito de fazer um levantamento do número de pessoas que já tinham de alguma forma algum conhecimento ou contato com a Física Quântica.

O professor antes de aplicar o teste comunicou aos alunos que aquilo não era uma avaliação onde eles teriam uma nota ao final. Também foi esclarecido a eles que as perguntas não tinham uma resposta certa ou errada, necessariamente. Com isso notou-se uma clara aceitação e conforto por parte dos alunos de fazerem o teste.

As perguntas não abordavam a parte conceitual ou teórica sobre a Mecânica Quântica, mas sim se o tema era de alguma forma familiar a eles. A intenção era saber quantos já tinham pelo menos ouvido falar sobre, mesmo que nada soubessem a respeito do assunto. E mesmo os que de alguma forma julgavam saber sobre o tema não seria necessário que respondessem nada específico sobre Mecânica Quântica. Para aqueles que se julgavam não ter tido nenhum contato com o tema em questão, ficava a opção de saber se eles tinham interesse sobre o assunto. A intenção de um esclarecimento antes de aplicar o teste era deixa-los bem à vontade para que as respostas fossem sinceras e que eles não se sentissem constrangidos seja qual fosse a resposta. Exemplo: se um aluno já tivesse lido qualquer revista, notícia ou artigo sobre mecânica quântica e entendido algo mesmo que bem superficial, que não se sentisse coagido ao responder ‘que conhecia o tema’ mesmo não se recordando muito bem o que leu ou não tendo condições de explicar o que entendeu. Assim como os alunos que nada sabem a respeito

não ficassem desconfortáveis em dizer que nada sabiam. Mas o principal do questionário era descobrir se os alunos que haviam jogado o produto guardavam alguma informação que o fizesse acreditar que possuía algum conhecimento sobre mecânica quântica.

6.2 – O Questionário

O questionário foi aplicado no mesmo colégio onde o produto já tinha sido aplicado, uma vez que o produto tem a finalidade de familiarizar o estudante do ensino básico com as ideias do mundo quântico. Era necessário testar os alunos que jogaram o produto para saber se o objetivo foi alcançado, se houve estabilidade cognitiva e em que nível ocorreu o aprendizado.

O teste foi aplicado em uma turma do 3° ano do ensino médio no ano seguinte em que o produto foi aplicado aos alunos. A turma de 3° ano já tinha participado da aplicação do produto no ano anterior quando ainda era do 2° ano do ensino médio, ou seja, eles já tiveram contato com o produto e a oportunidade de discutir sobre o tema com o professor. E agora, 6 meses depois, ao serem submetidos a esse teste o que estava em questão era observar a eficácia do produto em inserir conhecimentos da mecânica quântica e tentarmos ter uma conclusão do tipo de aprendizagem que tivemos com o produto.

6.3 – A Resposta

O questionário foi aplicado para aproximadamente 20 alunos do ensino médio, onde praticamente todos os alunos conheceram o produto, porém já havia passado mais de 6 meses, ou seja, o jogo foi apresentado a eles no ano letivo anterior.

O grupo que já havia jogado o produto foi avaliado com a intenção de sabermos o quanto o produto os fez assimilar algo sobre mecânica quântica. E as respostas, na sua maioria, foram similares. Grande parte dos alunos respondeu que já tinha ouvido falar sobre mecânica quântica, mesmo que não recordasse sobre o assunto ou não soubesse do que realmente se tratava (*apêndice 2.2*). Essa pergunta feita a eles tinha o objetivo de saber se pelo menos em algum momento em sua vivência já teriam escutado, lido ou visto algo que mencionava a mecânica quântica.

Um número significativo de alunos se dividiu em duas respostas; uma parte respondeu que sabia de alguma forma o que era mecânica quântica, mas não saberia explicar, e a outra parte respondeu que não sabia o que era, mas já tinha lido algo a respeito (apêndice 2.3). Aqui temos uma amostragem que nos leva a supor que em algum momento houve um interesse de parte dos alunos sobre o tema, pois eles mesmos por si só já tinham lido algo a respeito. E a outra metade que julgou saber o que era mecânica quântica, pode ter apresentado uma memória do jogo, uma aprendizagem que ocorreu de forma participativa ao interagir com o produto.

A respeito do "Gato de Schrödinger" a maioria das respostas foi negativa quanto ao conhecimento do tema ou uma resposta negativa acompanhada do interesse em saber sobre o mesmo. Poucos responderam que já tinham lido sobre o assunto e quase ninguém respondeu que sabia ou que sabia sobre o "gato" mas não teria condições de explicar. Fica aqui um questionamento sobre esse desconhecimento, pois o Gato de Schrödinger é o mais clássico exercício de imaginação atribuído a mecânica quântica. Talvez o assunto não tivesse sido abordado como deveria após a aplicação do produto ou o produto os levou a prestar mais atenção em outros detalhes, como, por exemplo, o mecanismo de criptografar uma mensagem.

As duas últimas respostas foram quase que unanimes, praticamente todos não sabiam o que era uma função de onda e praticamente todos sabiam o que era criptografia mas não saberiam explicar. A conclusão que podemos ter com essas duas últimas respostas é de que o termo que poderia ser mais facilmente encontrado no dia a dia, como criptografia, era de conhecimento. Já a função de onda, que é uma definição quântica não muito utilizada na rotina de um leigo, foi considerada algo desconhecido por quase todos. Mesmo os que diziam saber algo sobre mecânica quântica não sabiam dizer nada sobre função de onda. Levo a entender que o termo pode não ter sido bem trabalhado na aplicação do produto ou a dificuldade de abstração para compreender o que é uma função de onda faz com que o termo seja praticamente ignorado pelos alunos do ensino médio.

Com esse questionário tentamos avaliar qual foi a contribuição do produto na construção do conhecimento dos alunos a respeito da mecânica quântica. E de alguma forma identificar o tipo de aprendizagem que ocorreu na aplicação do jogo. De acordo

com a definição de Ausubel sobre aprendizagem significativa, é necessário dar significados ao novo conhecimento por interações com significados claros, estáveis e diferenciados já pré-existentes na estrutura cognitiva do aluno (Ausubel apud Moreira A.M. 2014. Cap 7).

O jogo, ao ser oferecido como forma de interação com os alunos, dá a eles uma pré-disposição para o aprendizado. Uma das condições para que o aluno aprenda de forma significativa é justamente ele apresentar pré-disposição para aprender, e o jogo deve ser um material de aprendizagem potencialmente significativo. Curiosamente e coincidentemente, o questionário foi aplicado bem em meio à semana em que estreou nos cinemas um filme que mencionou o mundo quântico. O filme era o fechamento de uma série de outros filmes em que as suas histórias se entrelaçavam, e a solução para o bem vencer o mal no filme era uma viagem no tempo, e, segundo o filme, isso era possível desde que se pudesse acessar o mundo quântico através de um portal quântico.

Apesar das extrapolações dos termos usados no filme de ficção, o que ficou bem claro foi a empolgação dos alunos ao retomar esse assunto devido à influencia do filme. Acredito que aqui os alunos estavam mais pré-dispostos a debater e aprender sobre o tema, mesmo aqueles que nada sabiam sobre o tema ou aqueles que já haviam lido algo a respeito.

APÊNDICE 1

Apêndice 1.1 - Cartela do Emissor

Mensagem	

Cor	Forma
Preto = 1	Bola = 1
Branco= 0	Quadrado=0

Impar	Par
1 - 3 - 5	2 – 4 - 6
Cor	Forma

Unidade Genética	Codificação
A	00
C	01
G	10
T	11

	Base	Macrobits	Informação	Checagem	CHAVE
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					
11					
12					
13					
14					
15					
16					
17					
18					
19					
20					

Chave		
Mensagem		
Mens.Criptografada		

Apêndice 1.2 - Cartela do Receptor

Mensagem	

Cor	Forma
Preto = 1	Bola = 1
Branco= 0	Quadrado=0

Impar	Par
1 - 3 - 5	2 – 4 - 6
Cor	Forma

Unidade Genética	Codificação
A	00
C	01
G	10
T	11

	Base	Macrobits	Informação	Checagem CHAVE
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				
18				
19				
20				

Chave		
Mens.Criptografada		
Mensagem		

APÊNDICE 2

Apêndice 2.1 – O questionário

MECÂNICA QUÂNTICA

1- Você já ouviu falar sobre Mecânica Quântica?
a) Não
b) Sim
c) Sim, mas não me recordo
d) Sim, mas não sei do que se trata
e) Não, mas gostaria de saber

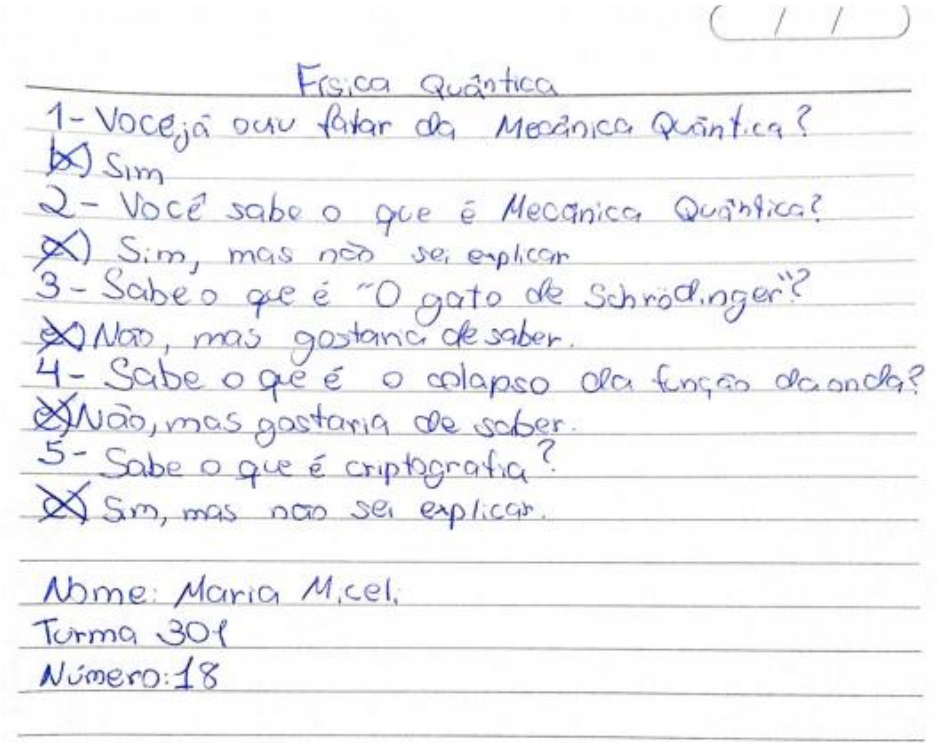
2- Você sabe o que é Mecânica Quântica?
a) Não
b) Sim
c) Sim, mas não sei explicar
d) Não, mas já li sobre o assunto
e) Não, mas gostaria de saber

3- Sabe o que é “O gato de Schrödinger”?
a) Não
b) Sim
c) Sim, mas não sei explicar
d) Não, mas já li sobre o assunto
e) Não, mas gostaria de saber

4- Sabe o que é o colapso da função de onda?
a) Não
b) Sim
c) Sim, mas não sei explicar
d) Não, mas já li sobre o assunto
e) Não, mas gostaria de saber

5- Sabe o que é Criptografia?
a) Não
b) Sim
c) Sim, mas não sei explicar
d) Não, mas já li sobre o assunto
e) Não, mas gostaria de saber

Apêndice 2.2 – Resposta do teste aluna 1



Física Quântica

1- Você já ouviu falar da Mecânica Quântica?
b) Sim

2- Você sabe o que é Mecânica Quântica?
c) Sim, mas não sei explicar

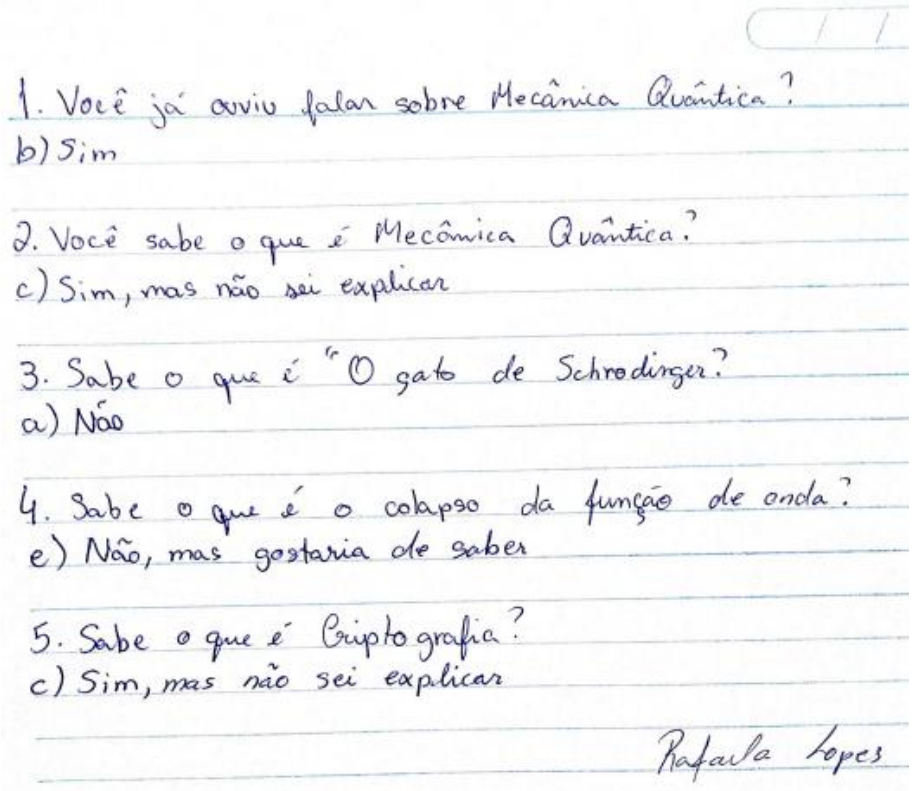
3- Sabe o que é "O gato de Schrödinger"?
a) Não, mas gostaria de saber.

4- Sabe o que é o colapso da função da onda?
e) Não, mas gostaria de saber.

5- Sabe o que é criptografia?
c) Sim, mas não sei explicar.

Nome: Maria M.cel.
Turma 301
Número: 18

Apêndice 2.3 – Resposta do teste aluna 2



1. Você já ouviu falar sobre Mecânica Quântica?
b) Sim

2. Você sabe o que é Mecânica Quântica?
c) Sim, mas não sei explicar

3. Sabe o que é "O gato de Schrodinger?
a) Não

4. Sabe o que é o colapso da função de onda?
e) Não, mas gostaria de saber

5. Sabe o que é Criptografia?
c) Sim, mas não sei explicar

Rafaela Lopes

APÊNDICE 3

O JOGO

3.1 - Introdução

O trabalho tem o objetivo de aplicar um jogo de transmissão segura de informações baseado na ideia da criptografia, e posteriormente utilizar a dinâmica do jogo para o aprendizado da Mecânica Quântica, utilizando como ferramenta a Criptografia Quântica. O jogo inicialmente tem como finalidade apresentar o conceito básico da criptografia para um melhor entendimento dos alunos, e posteriormente evoluir para o ensino da mecânica quântica.

A criptografia hoje atua em diversos aplicativos, sistemas bancários e sites compras pela internet, por exemplo, e por estar presente no cotidiano das pessoas é que seria interessante utiliza-la como produto de ensino de Física.

3.2 - Objetivo do Jogo:

O objetivo do jogo é a transmissão de uma mensagem secreta entre dois jogadores, ou dois grupos de jogadores, onde pessoas que assistam a essa transmissão não sejam capazes de identificar qual é o conteúdo da mensagem transmitida.

3.3 - Componentes do Jogo:

-Uma urna com diversos Macrobits

As formas são círculo e quadrado, as cores são preto e branco. Cada peça, independente do seu formato, tem uma face preta e a outra branca, conforme o exemplo abaixo.

■□●○■□●○■□●○■□●

-Uma régua suporte.

-Dois dados.

-Duas cartelas (uma Cartela Emissor e uma Cartela Receptor).

3.4 - Regras do Jogo:

O Professor cria a mensagem que será criptografada, guardando-a para si, e sorteia da urna uma sequência de Macrobits e os coloca na régua suporte, respeitando a sequência sorteada e a face que ficará virada para os jogadores.

Um jogador (emissor) cria aleatoriamente, jogando os dados, uma sequência de duas características do Macrobit. Sendo Forma para números pares e Cor para números impares, essa sequência preenche na Cartela a primeira coluna (BASE). O outro jogador (receptor) faz o mesmo em sua Cartela usando o seu dado.

O emissor recebe a régua suporte e retira da sequencia de Macrobits as características das peças de acordo com a sequencia da sua Base, preenchendo com essa característica a segunda coluna da cartela (Macrobit).

O receptor recebe a régua suporte do emissor e também preenche a coluna Macrobit da sua cartela de acordo com a sua Base.

Todos os jogadores devem respeitar a sequência e a face dos Macrobits sorteados pelo professor.

Cada jogador, tanto emissor como receptor, deve preencher a terceira coluna (Informação) com a informação binária do Macrobit de acordo com sua Base, ou seja, codifica a característica do Macrobit.

O receptor “canta” a sequência da sua base e o emissor diz “sim” caso a informação coincida com a do emissor e diz “não” quando não coincidir. Ambos jogadores preenchem a quarta coluna (Checagem) com “sim” e “não”.

Ambos jogadores em suas respectivas cartelas preenchem a quinta coluna da cartela (Chave) com a informação binária que coincidiram com um “sim”. Nessa última coluna, está a Chave que deverá criptografar a mensagem.

O procedimento deve ser repetido até que o número de bits coincidentes seja suficiente para criptografar toda a mensagem.

O Emissor recebe do Professor a mensagem secreta e a codifica para a linguagem binária, em seguida criptografa a mensagem com a chave e a entrega ao professor.

O professor entrega a mensagem secreta a todos, incluindo o receptor, e este último descriptografa a mensagem secreta com a chave que está em sua cartela (Cartela Receptor).

O professor confere as mensagens e as revela a todos.

3.5 - Como se constrói a Base:

Cada jogador preenche a primeira coluna da cartela jogando o dado e conferindo qual informação deverá ser usada no jogo conforme a tabela que se encontra na sua cartela:

Impar	Par
1 - 3 - 5	2 – 4 - 6
Cor	Forma

3.6 - Como se codificam as características do Macrobit:

A terceira coluna (informação) deve ser preenchida com a característica do Macrobit porém, na linguagem binária:

COR	FORMA
PRETO=1	BOLA=1
BRANCO=0	QUADRADO=0

3.7 - Como se codifica a mensagem:

A mensagem deve ser criada a partir de um alfabeto de 4 caracteres, pois assim, com apenas 2 Bits (0 e 1), podemos escrever qualquer “palavra” com esse alfabeto usando o código binário de maneira simples.

Ex: Alfabeto Genómico A T C G (bases nitrogenadas)

A	0	0
T	0	1
C	1	0
G	1	1

3.8 - Como se criptografa a mensagem:

Para se criptografar a mensagem secreta, inicialmente a mensagem deve estar codificada, em seguida usa-se a tabela operação lógica Xor e faz-se a criptografia da mensagem com a chave:

MENSAGEM = 1 0 1 0 1 1 0 1
CHAVE = 0 0 0 1 1 0 0 0
CRIPTOGRAFADA = 1 0 1 1 0 1 0 1

A	B	A#B
0	0	0
0	1	1
1	0	1
1	1	0

Para descriptografar a mensagem, basta usar novamente a chave e a tabela operação lógica Xor.

APÊNDICE 4 - Postulados da Mecânica Quântica.

Como dito no capítulo 3 a mecânica quântica tem em seus fundamentos sete postulados os quais são listados abaixo e acompanhados de uma sucinta descrição:

Postulado I (Existência do vetor de estado):

Associada ao movimento de uma partícula existe um vetor de estado $|\psi\rangle$ *que contém toda a informação sobre a partícula.*

A dualidade partícula-onda requer uma descrição ondulatória da matéria que contenha parâmetros corpusculares, como momento linear e energia, em seu bojo.

Postulado II (Operadores):

Toda grandeza física é representada por um operador hermetiano (ou observável), $\hat{O}$*, aplicado ao vetor de estado:* $\hat{O}|\psi\rangle = o|\psi\rangle$.

De certa maneira, os operadores também figuram na física clássica. Para se obter a velocidade de um ponto pertencente a uma corda vibrante, por exemplo, o que se deve fazer é aplicar uma derivada temporal à função que descreve a corda. A aplicação do operador ao vetor de estado resulta no auto-valor do problema.

Postulado III (Equação de Schrödinger):

A dinâmica temporal do vetor de estado $|\psi\rangle$ *é governada pela equação de Schrödinger*

$$\hat{H}|\psi\rangle = E|\psi\rangle$$

onde $\hat{H}$ *corresponde ao operador hamiltoniano do sistema e E é a energia da partícula.*

A equação de Schrödinger corresponde à aplicação do princípio da conservação de energia para o caso dos sistemas quânticos.

Postulado IV (Princípio da superposição):

Todo vetor de estado pode ser decomposto em termo dos auto-vetores associados ao um dado operador.

$$|\psi\rangle = \sum_{n=1}^{N} c_n |\phi_n\rangle$$

Este postulado origina o paradoxo do "gato de Schrödinger".

Postulado V (Colapso da função de Onda):

O processo de medida de uma partícula quântica provoca a redução do vetor de estado.

$$|\psi\rangle = \sum_{n} c_n |\phi_n\rangle \xrightarrow{colapso} |\phi_m\rangle$$

A discussão deste postulado foi feita no capítulo 3. A redução do vetor de estado ocorre de acordo com o observável em questão, ou seja, o auto-estado que resulta da medida depende do operador e o valor medido é o auto-valor correspondente ao auto-estado.

Postulado VI (Interpretação Probabilística):

A densidade de probabilidade de encontrar a partícula em um determinado auto-estado é dada pelo módulo quadrado da projeção do vetor de estado naquele auto-estado.

$$P_m = |\langle \phi_m | \psi \rangle|^2$$

Postulado VII (Partículas idênticas):

Um sistema quântico composto por bósons idênticos possui função de onda simétrica. Caso ele seja composto por férmions, a função de onda do sistema será antissimétrica.

Exemplo de aplicação:

Digamos que se deseja medir uma determinada grandeza física (definida por um operador $\hat{O}$) de uma partícula quântica descrita por um vetor de estado $|\psi\rangle$. Deve-se primeiramente decompor o vetor de estado em termos dos auto-estados do operador $\hat{O}$: $|\psi\rangle = \sum_{n=1}^{N} c_n |\phi_n\rangle$ em que os $|\phi_n\rangle$ são tais que $\hat{O}|\phi_n\rangle = o_n |\phi_n\rangle$. No instante da

medida tem-se o colapso do vetor de estado de forma que $|\psi\rangle = \sum_n c_n |\phi_n\rangle \xrightarrow{colapso} |\phi_m\rangle$ e o resultado da medida será o auto-valor o_m com probabilidade dada por $|\langle\phi_m|\psi\rangle|^2$

REFERENCIA BIBLIOGRÁFICA

- Vygotsky e Ausubel apud MOREIRA, M.A. **Teorias de aprendizagem.** 2. Ed. Ampl. - EPU: São Paulo, 2014. Cap7 e 11.
- BROCKINGTON, Guilherme PIETROCOLO, Mauricio. **Serão as regras da transposição didática aplicáveis ao conceito de física moderna?** In. Investigações em Ensino de Ciências. USP.São Paulo, 2005. 387-404p.
- BENNETT e BRASSARD.**Quantum cryptography:Public key distribution and coin tossing**. Theoretical Computer Science. In.1984.
- Charles C. Bonwell. **Active Learning: Creating Excitement in the Classroom.**2000. 2-17p.
- COHEN-TANNOUDJI, C.; DIU, B.; LALOë, F. **Quantum mechanics**. New York: John Wiley e Sons, (1977).
- MACEDO JUNIOR, M.A.V, PEREIRA, J.A.M. **Dissertação de mestrado "Tópicos atuais em física quântica: das ondas de matéria à realidade quântica**". IFRJ (2012)
- FEYNMAN,R.P**. Lições de Física.Física Quântica V3**.Porto Alegre, 2018.
- LEMOS, Manuel. **Criptografia, Números Primos e Algoritmos**. (2009)