

UNIVERSIDADE FEDERAL DO ESTADO DO RIO DE JANEIRO
PROGRAMA DE PÓS GRADUAÇÃO EM ENSINO DE FÍSICA
MESTRADO NACIONAL PROFISSIONAL EM ENSINO DE FÍSICA
POLO 30

Thiago Nunes Oliveira Cabral

Encriptamento Quântico no Ensino Médio Utilizando o Protocolo BB84

Rio de Janeiro
2026

Thiago Nunes Oliveira Cabral

Encriptamento Quântico no Ensino Médio Utilizando o Protocolo BB84

Dissertação apresentada ao Polo 30 do
Programa de Mestrado Nacional Profissional
em Ensino de Física da Unirio como
requisito parcial à obtenção do título de Mestre
em Ensino de Física. Área de concentração:
Ensino de Física.

Orientador: João Alberto Mesquita Pereira

Rio de Janeiro

2026

FICHA CATALOGRÁFICA

Catálogo informatizado pelo(a) autor(a)

NC117 Nunes Oliveira Cabral, Thiago
 Encriptamento Quântico no Ensino Médio Utilizando o
 Protocolo BB84 / Thiago Nunes Oliveira Cabral. -- Rio de
 Janeiro : UNIRIO, 2026.
 101

 Orientador: João Alberto Mesquita Pereira.
 Dissertação (Mestrado) - Universidade Federal do Estado
 do Rio de Janeiro, Programa de Pós-Graduação em Ensino de
 Física, 2026.

 1. Ensino de Física . 2. Criptografia quântica. 3.
 Protocolo BB84. I. Alberto Mesquita Pereira, João, orient.
 II. Título.



UNIRIO

UNIVERSIDADE FEDERAL DO ESTADO DO RIO DE JANEIRO

Mestrado Nacional Profissional em Ensino de Física - PROFIS-UNIRIO

DISSERTAÇÃO DE MESTRADO

Thiago Nunes Oliveira Cabral

Título: "Encriptamento Quântico no Ensino Médio Utilizando o Protocolo BB84"

Aprovada pela Banca Examinadora

Rio de Janeiro, 08/09/2026

Documento assinado digitalmente

gov.br

JOAO ALBERTO MESQUITA PEREIRA

Data: 08/09/2026 17:42:03-0300

Verifique em <https://validar.iti.gov.br>

Prof. Dr. João Alberto Mesquita Pereira
(orientador)

Documento assinado digitalmente

gov.br

IVAN DOS SANTOS OLIVEIRA JUNIOR

Data: 08/09/2026 19:33:54-0300

Verifique em <https://validar.iti.gov.br>

Prof. Dr. Ivan Santos Oliveira
(avaliador externo)

Prof. Dr. José Abdalla Helayel-Neto
(avaliador interno)

Documento assinado digitalmente

gov.br

JOSE ABDALLA HELAYEL NETO

Data: 08/09/2026 18:46:29-0300

Verifique em <https://validar.iti.gov.br>

DEDICATÓRIA

Dedico este trabalho às memórias dos meus avós, Durval Nunes Gomes e Alice Nunes Oliveira, por todo o carinho e dedicação que tiveram comigo em toda a sua vida, à memória do meu avô, Ivan Silva Leoni, pelos ensinamentos e valores que permanecem, e à minha avó, Wanda Maia Cabral, pelo amor, pelos ensinamentos e pela presença marcante em minha vida.

AGRADECIMENTOS

A realização deste trabalho só foi possível graças ao apoio de diversas pessoas que, cada um de sua maneira, contribuíram ao longo dessa trajetória.

Agradeço a Deus pela minha vida e por me dar forças para seguir em frente.

À minha mãe, Maria Nunes Oliveira Cabral, e ao meu pai, Edmo Cabral da Rocha Pinto, por serem meus modelos de vida e por me permitirem segui-la da melhor forma que eu poderia.

Ao meu irmão, Edmo Nunes Oliveira Cabral, por ser meu grande parceiro e estar ao meu lado em cada etapa da minha vida.

A minha noiva, Ingrid de Lima Gonçalves, pelo apoio constante, compreensão e incentivo, principalmente nos momentos mais desafiadores.

Aos colegas de curso, pelas trocas, conversas e apoio nessa jornada, tornando o percurso mais leve e enriquecedor.

Ao meu orientador, Professor Dr. João Alberto Mesquita Pereira, cuja disponibilidade, empenho e dedicação constante tem sido uma referência na minha formação acadêmica.

O presente trabalho foi realizado com o apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – Brasil (CAPES) – código de financiamento 001.

EPÍGRAFE

“O que podemos observar não é a natureza em si, mas a natureza exposta ao nosso método de questionamento.”

- Werner Heisenberg

RESUMO

Este trabalho tem como objetivo investigar a transmissão segura de informações a partir dos fundamentos da mecânica quântica, usando para isso um jogo didático baseado no protocolo BB84, propondo, desta forma, uma abordagem didática que favoreça sua compreensão no contexto do ensino de física no Ensino Médio. A pesquisa fundamenta-se na Teoria da Aprendizagem Significativa de David Ausubel, na perspectiva sociocultural de Lev Vygotsky e na concepção dialógica de Paulo Freire, considerando a valorização dos conhecimentos prévios, da interação social e da construção crítica do conhecimento como elementos centrais do processo de ensino e aprendizagem. Inicialmente, são apresentados elementos da teoria da informação e princípios quânticos relacionados à medição e à escolha de bases. Como metodologia, desenvolve-se um jogo educativo baseado no uso de macrobits, que simula o processo de distribuição de chaves quânticas, incluindo a preparação, transmissão e medição de estados. A proposta foi aplicada a uma turma experimental e comparada a uma abordagem tradicional, por meio de pré e pós-testes e registros observacionais. Os resultados indicam um maior engajamento, participação e compreensão conceitual dos alunos que participaram da atividade lúdica, evidenciando o potencial do jogo didático para favorecer a aprendizagem dos conceitos envolvidos. Conclui-se que a utilização de modelos didáticos inspirados na Mecânica Quântica, fundamentados nos pressupostos de Ausubel, Vygotsky e Freire, contribui para a aprendizagem significativa de temas contemporâneos da Física, favorecendo a construção colaborativa do conhecimento, o desenvolvimento da autonomia dos estudantes e a aproximação entre conceitos abstratos e experiências concretas.

Palavras-chave: Ensino de Física; criptografia quântica; macrobits; segurança da informação; computação quântica; Mecânica Quântica; Protocolo BB84.

ABSTRACT

This study aims to investigate the secure transmission of information based on the principles of quantum mechanics by employing an educational game based on the BB84 protocol, thereby proposing a teaching approach that facilitates the understanding of these concepts in the context of high school physics education. The research is grounded in David Ausubel's Theory of Meaningful Learning, Lev Vygotsky's sociocultural perspective, and Paulo Freire's dialogical approach, emphasizing the value of prior knowledge, social interaction, and the critical construction of knowledge as central elements of the teaching and learning process. Initially, the study presents elements of information theory and quantum principles related to measurement and the choice of measurement bases. As a methodological approach, an educational game based on the use of macrobits was developed to simulate the quantum key distribution process, including the preparation, transmission, and measurement of quantum states. The proposed activity was implemented with an experimental group and compared with a traditional teaching approach through the application of pre- and post-tests and observational records. The results indicate greater student engagement, participation, and conceptual understanding among those who took part in the game-based activity, highlighting the potential of the educational game to enhance the learning of the concepts involved. It is concluded that the use of educational models inspired by quantum mechanics, grounded in the theoretical assumptions of Ausubel, Vygotsky, and Freire, contributes to the meaningful learning of contemporary physics topics by fostering collaborative knowledge construction, promoting student autonomy, and bridging the gap between abstract concepts and concrete experiences.

Keywords: Physics teaching; Quantum cryptography; macrobits; information security; quantum computing; quantum mechanics; BB84 Protocol.

SUMÁRIO

1.	Introdução	12
2.	Revisão Bibliográfica	15
2.1	O ensino de Física Moderna e Contemporânea na Educação Básica	15
2.2	O ensino da Mecânica Quântica no Ensino Médio	15
2.3	A criptografia quântica como tema de ensino	16
2.4	Jogos didáticos no Ensino de Física	17
2.5	Trabalhos relacionados ao protocolo BB84	17
2.6	A contribuição da presente pesquisa	18
2.7	Análise de trabalhos correlatos.....	19
2.7.1.	Inserindo elementos da criptografia quântica no Ensino Médio – Fabrício Damasceno Belisário	19
2.7.2	Introdução à Criptografia Quântica – Rigolin e Rieznik (2005)	20
2.7.3	A Física do Tunelamento Quântico: uma proposta de organizador prévio para o Ensino Médio.....	20
2.8	Análise de trabalhos correlatos.....	21
3.	Resumo histórico e fundamentos da criptografia quântica.....	23
4.	Fundamentação Teórica.....	25
4.1	Teorias da Aprendizagem.....	25
4.1.1	A importância das teorias de aprendizagem no Ensino de Física.....	25
4.1.2	A teoria histórico-cultural de Lev Vygotsky	25
4.1.3	Mediação pedagógica	26
4.1.4	Instrumentos e signos	27
4.1.5	Funções Psicológicas Superiores.....	27
4.1.6	Zona de Desenvolvimento Proximal	28
4.1.7	Nível de Desenvolvimento Real e Nível de Desenvolvimento Potencial	29
4.1.8	A internalização como processo de aprendizagem.....	29
4.1.9	A internalização como processo de aprendizagem.....	30
4.1.10	A pedagogia crítica de Paulo Freire	30
4.1.11	O diálogo como princípio pedagógico.....	31
4.1.12	Aprendizagem Significativa de Ausubel e suas contribuições para o ensino de Mecânica Quântica	31
4.1.13	Articulação entre Vygotsky, Paulo Freire e o Produto Educacional	33
4.2	Teorias Quânticas	34
4.2.1	Introdução conceitual de mecânica quântica	34
4.2.2	O Princípio da incerteza de Heisenberg	35
4.2.3	O Princípio da Superposição de Autoestados.....	35
4.2.4	O Processo de Medição e o Colapso do Vetor de Estado.....	36
4.2.5	Superposição, Colapso e Segurança na Criptografia Quântica	36
4.3	Segurança da informação.....	37
4.3.1	Transmissão de mensagens.....	37
4.3.2	Macrobit	40
4.3.3	O uso do macrobit na criptografia do jogo	45
5.	Metodologia	47
5.1	Tipo de pesquisa	47
5.2	Contexto da pesquisa	47

5.3 Instrumentos de coleta de dados	48
5.4 Desenvolvimento da sequência didática.....	48
5.5 Procedimentos de análise dos dados.....	49
5.6 Aspectos éticos	49
5.7 Proposta didática	50
6. Avaliação	56
7. Aplicação do produto.....	58
7.1. Dia da dinâmica.....	58
7.2 Análise da compatibilidade das bases de medida.....	60
7.3 Dia da aula tradicional.....	61
8. Resultados.....	64
8.1 Aplicação do pré-teste	64
8.1.1 Resultados do pré-teste	64
8.1.2 Análise dos resultados	66
8.2 Aplicação do pós-teste.....	68
8.2.1 Resultados do pós-teste	69
8.2.2 Análise dos resultados	71
9. Conclusão	75
10. Referências Bibliográficas.....	77
APÊNDICE: PRODUTO EDUCACIONAL	79
1. Introdução	81
2. Fundamentação Teórica.....	82
2.1 Ensino de Física Moderna no Ensino Médio	82
2.2 Referencial pedagógico	82
2.3 Conceitos quânticos.....	83
3. O Macrobit.....	84
4. O jogo do encriptamento quântico BB84	85
4.1 Objetivos do jogo	85
4.2 Público-alvo.....	85
4.3 Materiais necessários	85
4.4 Organização da turma.....	86
4.5 Etapas do jogo	86
5. Aplicação em Sala de Aula.....	87
5.1 Tempo estimado	87
5.2 Apresentação e regras do jogo.....	87
5.3 Desenvolvimento da dinâmica	87
5.4 Discussões conceituais	88
5.5 Resultados finais.....	88
6. Avaliação da Aprendizagem.....	89
6.1 Avaliação diagnóstica.....	89
6.2 Avaliação durante o jogo.....	89
6.3 Avaliação final.....	89
6.4 Sugestões de questionamentos.....	90
7. Considerações Finais	91
8. Referências	92
APÊNDICE A: Teste pré-produto	93
APÊNDICE B: Teste pós-produto.....	96
APÊNDICE C: Tabela para o Emissor.....	99
APÊNDICE D: Tabela para o Receptor	100

1. Introdução

A Física Moderna representa uma das maiores revoluções científicas da história ao modificar profundamente a compreensão acerca da natureza da matéria, da energia e das interações fundamentais do universo. Entre seus diversos campos de estudo, a Mecânica Quântica destaca-se não apenas por sua relevância científica, mas também pelas inúmeras aplicações tecnológicas desenvolvidas nas últimas décadas, como a computação quântica, a criptografia quântica, a comunicação segura e os sensores de alta precisão. Esses avanços vêm transformando diversos setores da sociedade contemporânea, tornando imprescindível a aproximação desses conhecimentos da Educação Básica.

Apesar do crescente aumento da importância, o ensino da Física Moderna e Contemporânea ainda enfrenta inúmeros desafios nas escolas brasileiras. Em grande parte das instituições de Ensino Médio, os conteúdos permanecem concentrados na Física Clássica, enquanto temas relacionados à Física Moderna e à Física Contemporânea costumam ser tratados de forma superficial ou, muitas vezes, sequer são abordados. Entre os fatores que contribuem para esse cenário destacam-se a elevada abstração dos conceitos envolvidos, a insuficiência de materiais didáticos específicos, a limitação da carga horária e a insegurança de muitos professores diante de conteúdos cuja formação inicial frequentemente não contemplou abordagens pedagógicas aprofundadas.

Além dessas dificuldades, observa-se que muitos estudantes desenvolvem uma percepção da Física como uma disciplina excessivamente matemática e distante das aplicações tecnológicas presentes em seu cotidiano. Essa visão reduz o interesse pela área e dificulta a construção de aprendizagens significativas, especialmente quando o conteúdo exige elevado grau de abstração, como ocorre em Mecânica Quântica. Nesse contexto, torna-se necessário desenvolver estratégias metodológicas capazes de aproximar conceitos complexos da realidade dos estudantes, favorecendo a construção do conhecimento por meio de experimentação, da interação e da resolução de problemas.

Entre as aplicações mais relevantes da Mecânica Quântica encontra-se a criptografia quântica, cuja finalidade consiste em possibilitar a transmissão segura de informações utilizando propriedades fundamentais dos sistemas quânticos. Diferentemente dos métodos clássicos de criptografia, cuja segurança depende principalmente da dificuldade computacional de quebra de códigos, a criptografia quântica fundamenta-se nas próprias leis da natureza, especialmente na impossibilidade de realizar medições sem provocar alterações detectáveis no sistema físico.

O protocolo BB84, proposto por Charles Bennet e Gilles Brassard em 1984, constitui o primeiro protocolo de distribuição de chaves (Quantum Keys Distribution – QKD) e permanece, até os dias atuais, como um dos principais modelos utilizados para introduzir os fundamentos da comunicação quântica segura. Sua simplicidade conceitual, aliada ao elevado potencial didático, torna-o especialmente adequado para propostas educacionais voltadas ao Ensino Médio.

Entretanto, a compreensão do protocolo BB84 exige o domínio de conceitos abstratos da Mecânica Quântica, como estados quânticos, superposição, bases de medição, preparação de estados, colapso do vetor de estado e probabilidades associadas às medidas. Esses conceitos, quando apresentados exclusivamente por meio de formalismos matemáticos, podem dificultar

significativamente a aprendizagem dos estudantes da Educação Básica. Dessa forma, torna-se necessário desenvolver recursos didáticos que permitam representar esses fenômenos por meio de analogias e modelos físicos acessíveis, preservando o rigor conceitual sem exigir conhecimentos matemáticos avançados.

Foi com esse propósito que se desenvolveu o macrobit, um dispositivo didático concebido para representar, em escala macroscópica, aspectos conceituais associados aos qubits utilizados na Mecânica Quântica. Embora não reproduza fenômenos genuinamente quânticos, o macrobit permite estabelecer analogias que auxiliam na compreensão da influência da escolha da base de medição, da representação de estados e do compartilhamento de informações.

A utilização de modelos analógicos constitui uma estratégia amplamente empregada no Ensino de Ciências, sobretudo quando os fenômenos estudados não podem ser observados diretamente. Nesse sentido, o macrobit assume o papel de mediador entre o conhecimento científico e a aprendizagem dos estudantes, permitindo que conceitos altamente abstratos sejam representados por meio de objetos concretos, manipuláveis e visualmente acessíveis.

A presente pesquisa propõe a utilização de um jogo didático fundamentado no protocolo BB84, no qual os estudantes participam ativamente do processo de codificação, transmissão, compartilhamento de chaves e decodificação de mensagens utilizando macrobits. Dessa maneira, busca-se favorecer não apenas a compreensão dos princípios da criptografia quântica, mas também estimular o interesse pela Física Moderna por meio de uma abordagem investigativa, colaborativa e contextualizada.

A estratégia proposta é um jogo didático, desenvolvido para ser aplicado em duplas de alunos. Um dos estudantes assume o papel de emissor, responsável por encriptar uma mensagem curta (três letras), enquanto o outro deve decifrá-la utilizando os princípios do protocolo BB84. Ao simular a transmissão e leitura de qubits por meio de representações simbólicas (macrobits), os alunos são levados a compreender conceitos complexos de forma prática e lúdica. Essa abordagem tem como uma das referências a dissertação de mestrado de Fabrício Damasceno Belisário, que orientou o uso de ferramentas pedagógicas, como os macrobits, para facilitar o ensino de princípios da criptografia quântica e do comportamento de sistemas quânticos, proporcionando uma maneira mais intuitiva e acessível de explorar esses conceitos. Aquele trabalho restringiu-se a apresentar o macrobit, deixando uma oportunidade muito interessante para esta dissertação que irá trazer uma evolução importante que é o uso do macrobit contextualizado em um jogo tendo a criptografia BB84 como temática principal. A escolha pela criptografia quântica se justifica não apenas pelo seu apelo tecnológico e interdisciplinar, mas também por seu papel fundamental nas discussões contemporâneas sobre segurança digital, privacidade de dados e tecnologia de ponta — temas que dialogam diretamente com o cotidiano dos jovens.

A proposta pedagógica desenvolvida nesta dissertação fundamenta-se nos pressupostos da teoria sociointeracionista de Lev Vygotsky e na pedagogia crítica de Paulo Freire. Sob a perspectiva vygotskyana, considera-se que a aprendizagem ocorre por meio das interações sociais mediadas por instrumentos, signos e pela atuação do professor, possibilitando que os estudantes avancem de seu nível de desenvolvimento real para sua Zona de Desenvolvimento Proximal. Paralelamente, a perspectiva freireana orienta a construção de um ambiente de aprendizagem baseado no diálogo, na problematização da realidade e na participação ativa dos estudantes como sujeitos do processo educativo.

Assim, o jogo proposto deixa de ser apenas uma atividade lúdica para constituir-se como um instrumento de mediação pedagógica capaz de favorecer a construção coletiva do

conhecimento científico. Durante sua aplicação, os estudantes são convidados a levantar hipóteses, discutir estratégias, justificar decisões, interpretar resultados e estabelecer relações entre os fenômenos observados e os conceitos da Mecânica Quântica, promovendo uma aprendizagem mais significativa.

Diante desse contexto, esta pesquisa busca responder ao seguinte problema de investigação: Como a utilização de um jogo didático baseado no protocolo BB84, utilizando o macrobit como recurso pedagógico, pode contribuir para a aprendizagem de conceitos introdutórios de Mecânica Quântica e criptografia quântica por estudantes do Ensino Médio?

Assim, o objetivo geral desta pesquisa é investigar as contribuições de um jogo didático inovador fundamentado no protocolo BB84, utilizando o macrobit como recurso pedagógico, para o ensino e aprendizagem de conceitos introdutórios de Mecânica Quântica e criptografia quântica no Ensino Médio.

De maneira mais específica, a pesquisa se propõe a desenvolver um produto educacional baseado no protocolo BB84 adequado ao contexto do Ensino Médio, utilizando o macrobit como recurso didático para representar conceitos fundamentais da Mecânica Quântica, favorecendo a compreensão dos conceitos de superposição, bases de medição, preparação de estados, colapso do vetor de estado e compartilhamento seguro de chaves criptográficas.

Além disso, o presente trabalho pretende analisar as potencialidades e limitações da utilização do jogo como estratégia de ensino, relacionando os resultados obtidos com os pressupostos teóricos de Lev Vygotsky e Paulo Freire, discutindo suas contribuições para o ensino de Física Moderna.

Para isso, este trabalho está organizado em capítulos que contemplam inicialmente a revisão da literatura relacionada ao ensino de Física Moderna, à criptografia quântica e às teorias educacionais que fundamentam a pesquisa. Em seguida, apresenta-se a fundamentação física necessária para a compreensão do protocolo BB84 e do macrobit. Posteriormente são descritos os procedimentos metodológicos adotados, a aplicação do produto educacional, a análise dos resultados obtidos e as considerações finais. Ao término do trabalho é apresentado, como apêndice, o Produto Educacional completo, permitindo sua utilização por outros professores da Educação Básica.

A Base Nacional Comum Curricular (BNCC, 2018) estabelece que os estudantes devem desenvolver competências que lhes permitam compreender o papel da ciência e da tecnologia na sociedade. Nesse cenário, a inserção da Física Moderna e Contemporânea — ainda pouco explorada nas escolas — é fundamental para uma formação científica crítica e atualizada.

Este trabalho está, portanto, alinhado aos objetivos da BNCC e se propõe a investigar e aplicar estratégias pedagógicas eficazes para introduzir o conceito de encriptamento quântico no Ensino Médio de maneira acessível, lúdica e conceitualmente sólida. Acreditamos que, ao integrar jogos, teoria quântica e abordagens pedagógicas emancipatórias, seja possível promover a curiosidade, a motivação e o protagonismo dos alunos no processo de aprendizagem.

2. Revisão Bibliográfica

2.1 O ensino de Física Moderna e Contemporânea na Educação Básica

Nas últimas décadas, muitos pesquisadores tem pontuado a necessidade de introduzir conteúdos de Física Moderna e Contemporânea na Educação Básica, em virtude da crescente presença de tecnologias fundamentadas nesse conhecimento no cotidiano da sociedade. Dispositivos eletrônicos, sistemas de comunicação, sensores, tecnologias médicas e métodos de segurança digital são exemplos de aplicações cuja compreensão exige a inda que de forma introdutória, conceitos desenvolvidos a partir da Mecânica Quântica.

Apesar desse cenário, o currículo tradicional do Ensino Médio permanece fortemente centrado na Física Clássica. Em muitos casos, os conteúdos de Física Moderna são abordados apenas ao final do terceiro ano, quando há tempo disponível, ou são completamente omitidos em razão da necessidade de preparação para exames vestibulares, principalmente o Exame Nacional do Ensino Médio (ENEM). Como consequência, inúmeros estudantes concluem a Educação Básica sem qualquer contato contínuo com conceitos que fundamentam parte significativa da tecnologia contemporânea.

Pesquisadores da área de Ensino de Física apontam que essa lacuna decorre de diferentes fatores, entre eles o elevado grau de abstração dos conceitos quânticos, a formação insuficiente de parte dos professores, a escassez de materiais didáticos apropriados e a dificuldade de desenvolver atividades experimentais que permitam representar fenômenos microscópicos em sala de aula, são os que mais se destacam.

Nesse cenário, aumenta o interesse por metodologias capazes de tornar esses conteúdos mais acessíveis, utilizando recursos didáticos, analogias, modelos físicos, simulações computacionais, jogos e atividades investigativas que aproximam a teoria da realidade vivenciada pelos estudantes.

2.2 O ensino da Mecânica Quântica no Ensino Médio

A literatura especializada mostra que o ensino da Mecânica Quântica na Educação Básica não deve buscar a formalização matemática característica dos cursos superiores, mas priorizar a compreensão conceitual dos fenômenos envolvidos e sua correlação com elementos do cotidiano. Essa perspectiva permite que os estudantes construam modelos explicativos acerca

da natureza quântica da matéria antes do aprofundamento matemático, favorecendo uma aprendizagem mais significativa e duradoura.

Alguns trabalhos desenvolvidos no âmbito do Mestrado Nacional Profissional em Ensino de Física (MNPEF) tem proposto sequências didáticas voltadas à introdução de conceitos como dualidade onda-partícula, efeito fotoelétrico, quantização da energia, superposição de estados e interpretação probabilística das medidas quânticas. Em comum, essas pesquisas apontam que atividades baseadas em experimentação, resolução de problemas e modelagem favorecem maior envolvimento dos estudantes quando comparadas às abordagens exclusivamente expositivas.

Entretanto, observa-se que ainda são poucos os trabalhos que abordam especificamente a criptografia quântica como tema central do processo de ensino-aprendizagem, especialmente utilizando materiais manipuláveis desenvolvidos com materiais de fácil acesso, e até mesmo recicláveis, para estudantes do Ensino Médio.

2.3 A criptografia quântica como tema de ensino

A criptografia é um assunto interdisciplinar que estabelece relações entre Física, Matemática, Ciência da Computação e Tecnologia da Informação. Sua crescente importância e presença na sociedade digital torna esse tema especialmente atrativo para estudantes do Ensino Médio, uma vez que envolve aplicações diretamente relacionadas ao cotidiano, como proteção de mensagens, transações bancárias, armazenamento de dados e segurança das comunicações digitais.

Com o desenvolvimento e a evolução da computação quântica, diversos pesquisadores passaram a investigar métodos de comunicação cuja segurança não dependesse apenas da dificuldade computacional de resolver determinados problemas matemáticos, mas das próprias leis da Mecânica Quântica. Nesse contexto surgiu a Distribuição Quântica de Chaves (Quantum Key Distribution – QKD), cuja proposta consiste em compartilhar chaves de criptográficas utilizando estados quânticos capazes de revelar qualquer tentativa de interceptação da comunicação.

Entre os protocolos existentes, o BB84 permanece como o mais difundido em pesquisas acadêmicas e aplicações experimentais, devido à simplicidade de sua estrutura e ao forte

embasamento físico que oferece para a introdução dos conceitos fundamentais da informação quântica.

Sob a perspectiva educacional, o protocolo BB84 apresenta um alto potencial didático por permitir que conceitos como preparação de estados, escolha de bases de medição, superposição, probabilidade e perturbação causada pela medida sejam discutidos de forma integrada em uma única atividade pedagógica.

2.4 Jogos didáticos no Ensino de Física

O uso de jogos didáticos tem sido amplamente investigado como estratégia para promover maior participação dos estudantes no processo de aprendizagem. Em oposição ao modelo transmissivo tradicional, os jogos favorecem a construção coletiva do conhecimento, estimulando a tomada de decisões, a resolução de problemas, a comunicação entre os participantes e a elaboração de hipóteses.

No Ensino de Física, diferentes pesquisas relatam ganhos relacionados ao aumento da motivação, da participação em sala de aula e da aprendizagem conceitual quando atividades lúdicas são planejadas de forma articulada aos objetivos educacionais. Contudo, a literatura também destaca que o jogo, isoladamente, não garante aprendizagem. Sua eficácia depende da mediação do professor, das discussões realizadas durante a atividade e da relação estabelecida entre a experiência vivenciada e os conceitos científicos envolvidos.

Essa perspectiva aproxima-se das contribuições de Lev Vygotsky, ao reconhecer que a aprendizagem ocorre mediante interações sociais mediadas por instrumentos culturais, e da pedagogia de Paulo Freire, ao compreender o estudante como sujeito ativo da construção do conhecimento.

2.5 Trabalhos relacionados ao protocolo BB84

A revisão da literatura evidencia que a maior parte das pesquisas envolvendo o protocolo BB84 concentra-se em aspectos físicos, matemáticos ou computacionais, voltados ao desenvolvimento de sistemas de comunicação quântica. Quando analisadas as pesquisas

direcionadas ao Ensino Médio, observa-se um número significativamente menor de propostas didáticas.

Grande parte desses trabalhos utiliza simulações computacionais, animações ou atividades baseadas em softwares especializados. Embora essas ferramentas apresentem elevado potencial pedagógico, sua utilização pode ser limitada pela infraestrutura disponível nas escolas e pelo acesso dos estudantes aos recursos tecnológicos necessários.

Em contraste, a utilização de materiais manipuláveis ainda parece de forma bastante restrita na literatura, especialmente aqueles capazes de representar, por analogia, conceitos fundamentais da Mecânica Quântica sem recorrer à complexidade matemática característica do ensino superior.

2.6 A contribuição da presente pesquisa

A proposta desenvolvida neste trabalho diferencia-se das pesquisas anteriormente descritas ao utilizar um dispositivo didático original – denominado macrobit – como elemento central de um jogo inspirado no protocolo BB84. Em vez de recorrer exclusivamente a simulações computacionais ou apresentações expositivas, a atividade permite que os estudantes manipulem fisicamente representações das diferentes bases de medição, vivenciando o processo de compartilhamento de chaves criptográficas de forma concreta e colaborativa.

Outra contribuição relevante consiste na integração entre os fundamentos da Mecânica Quântica e referenciais consolidados na área de Ensino de Ciências, especialmente a teoria sociointeracionista de Lev Vygotsky e a pedagogia crítica de Paulo Freire. Essa articulação amplia o alcance da proposta ao compreender que a aprendizagem dos conceitos científicos ocorre mediante processos de interação social, mediação pedagógica, problematização e construção coletiva do conhecimento.

Além disso, diferentemente de trabalhos que abordam apenas a descrição conceitual do protocolo BB84, esta pesquisa propõe um Produto Educacional passível de reprodução em

escolas de Educação Básica, utilizando materiais de baixo custo e procedimentos compatíveis com a realidade da maioria das instituições de ensino brasileiras.

2.7 Análise de trabalhos correlatos

2.7.1. Dissertação de mestrado e trabalhos apresentados em conferências

Entre os trabalhos mais próximos da presente pesquisa destacam-se a dissertação de Fabrício Damasceno Belisário, intitulada “Inserindo elementos da criptografia quântica no Ensino Médio”, orientada pelo prof. João A M Pereira, (BELISARIO, 2019). O trabalho apresenta uma sequência didática baseada no protocolo BB84 utilizando a polarização de fótons como elemento central para introduzir conceitos fundamentais da criptografia quântica aos estudantes do Ensino Médio. A proposta culmina na apresentação do macrobit como forma de simular a medição quântica, permitindo que os alunos compreendam a relação entre bases de medição, transmissão de informações e segurança das comunicações. A aplicação do jogo não foi realizada. A utilização do macrobit foi limitada à introdução de conceitos de mecânica quântica.

Os resultados apresentados pelo autor indicam elevado potencial motivados da atividade, favorecendo a participação dos estudantes e a compreensão inicial dos conceitos relacionado ao protocolo BB84. A utilização de uma abordagem lúdica mostrou-se eficiente para reduzir parte da abstração normalmente associada à Mecânica Quântica, tornando o conteúdo mais acessível aos alunos da Educação Básica. Entretanto, a proposta fundamenta-se predominantemente na utilização da polarização dos fótons como analogia para os qubits, permanecendo mais próxima do modelo físico original do protocolo BB84. O arcabouço conceitual envolvido, foi também apresentado em conferência de nível nacional (PEREIRA, 2022) e em artigo publicado na Revista do Professor de Física (PEREIRA, 2024).

A presente pesquisa diferencia-se por introduzir o macrobit como um novo recurso didático macroscópico, concebido especificamente para representar a escolha de bases de medição sem depender da manipulação de fenômenos ópticos. Além disso, o presente trabalho amplia a discussão pedagógica ao fundamentar a proposta nas teorias de Lev Vygotsky e Paulo Freire,

estabelecendo uma articulação mais explícita entre o produto educacional e referenciais contemporâneos da aprendizagem.

2.7.2 Introdução à Criptografia Quântica – Rigolin e Rieznik (2005)

Outro trabalho relevante é o artigo “Introdução à Criptografia Quântica”, publicado por Gustavo Rigolin e Andrés Aníbal Rieznik na Revista Brasileira de Ensino de Física. Embora não construa uma pesquisa voltada diretamente para a Educação Básica, esse trabalho apresenta uma descrição detalhada dos principais protocolos de distribuição quântica de chaves, especialmente o BB84, utilizando uma linguagem acessível para estudantes de graduação em Física. O artigo descreve os fundamentos físicos que garantem a segurança da comunicação quântica, discutindo aspectos relacionados à polarização de fótons, escolha de bases de medição, tentativa de espionagem e detecção de interceptações.

A principal contribuição dessa publicação reside na sistematização dos fundamentos conceituais da criptografia quântica, oferecendo o suporte teórico necessário para a elaboração de propostas didáticas inspiradas nesses protocolos. Entretanto, seu foco permanece na apresentação formal da teoria física, não contemplando estratégias metodológicas específicas para o Ensino Médio nem recursos didáticos voltados à aprendizagem escolar.

Em contraste, o presente trabalho busca transformar esses conceitos em uma experiência pedagógica concreta, utilizando um jogo didático e o macrobit como instrumento de mediação entre o conhecimento científico e a realidade dos estudantes. Dessa forma, procura-se reduzir a distância entre a teoria acadêmica da criptografia quântica e sua efetiva inserção na Educação Básica.

2.7.3 A Física do Tunelamento Quântico: uma proposta de organizador prévio para o Ensino Médio

Embora aborde outro fenômeno da Mecânica Quântica, a dissertação “A Física do Tunelamento Quântico: uma proposta de organizador prévio para o Ensino Médio”, desenvolvida no âmbito do MNPEF, apresenta contribuições importante para o ensino de Física Moderna ao propor estratégias metodológicas voltadas à introdução de conceitos quânticos em nível médio. O trabalho utiliza organizadores prévios como instrumento para favorecer a

aprendizagem significativa de conteúdos caracterizados por elevado grau de abstração, aproximando conceitos científicos da realidade dos estudantes.

Os resultados indicam que a utilização de recursos pedagógicos cuidadosamente planejados contribui para reduzir dificuldades conceituais frequentemente observadas quando conteúdos de Mecânica Quântica são apresentados exclusivamente por meio de formalismos matemáticos. Além disso, a pesquisa reforça a importância da mediação docente na construção de significados pelos estudantes durante o processo de aprendizagem.

Este trabalho compartilha essa preocupação com a transposição didática dos conceitos quânticos, mas diferencia-se ao utilizar um jogo colaborativo fundamentado no protocolo BB84 e um dispositivo didático original, o macrobit, como principal instrumento de mediação. Enquanto o trabalho sobre tunelamento concentra-se na compreensão de um fenômeno específico da Mecânica Quântica, esta pesquisa busca introduzir conceitos relacionados à informação quântica, à segurança digital e à criptografia, ampliando as possibilidades de contextualização tecnológica do ensino de Física.

2.8 Análise de trabalhos correlatos

A análise dos trabalhos revisados permite identificar uma tendência crescente de inserção da Física Moderna e Contemporânea na Educação Básica por meio de metodologias ativas, recursos manipuláveis, simulações computacionais e jogos didáticos. Observa-se, entretanto, que ainda são relativamente escassas as propostas voltadas especificamente ao ensino de criptografia quântica no Ensino Médio, sobretudo aquelas fundamentadas simultaneamente em referenciais consolidados da área de Ensino de Física e em teorias educacionais.

Nesse contexto, a presente pesquisa procura contribuir para o avanço dessa linha de investigação ao propor um Produto Educacional que articula fundamentos da Mecânica Quântica, o protocolo BB84, um recurso didático original (macrobit) e referenciais pedagógicos baseados em Lev Vygotsky e Paulo Freire. Tal interação busca não apenas favorecer a compreensão conceitual dos estudantes, mas também promover uma aprendizagem mediada,

colaborativa e contextualizada, aproximando conhecimentos científicos contemporâneos da realidade escolar.

3. Resumo histórico e fundamentos da criptografia quântica

O desenvolvimento da mecânica quântica no século XX representou uma ruptura paradigmática na história da ciência. Conceitos como indeterminação, superposição, colapso do vetor de estado e não localidade desafiaram a visão determinista clássica e abriram caminho para novas interpretações sobre a natureza da realidade física. Com esses avanços, tornou-se possível imaginar tecnologias antes impensáveis, entre elas a computação quântica e a criptografia quântica.

Essas aplicações surgiram ainda nos debates conceituais sobre a natureza da medição quântica. Experimentos mentais como o Gato de Schrödinger, proposto em 1935, exemplificam a característica paradoxal do mundo quântico. Nesse experimento, um sistema permanece em uma superposição de estados — vivo e morto simultaneamente — até que uma observação colapse o vetor de estado, revelando apenas uma das possibilidades. Esse paradoxo, apesar de idealizado, aponta para um princípio central: a medição afeta o estado do sistema.

A criptografia quântica surgiu a partir dessa ideia fundamental: se um sistema físico é utilizado para transmitir informação, qualquer tentativa de medi-lo indevidamente altera seu estado. Essa propriedade é a base da segurança incondicional dos protocolos quânticos. Enquanto os métodos clássicos de encriptação dependem de chaves matemáticas que podem ser quebradas com poder computacional suficiente, a criptografia quântica baseia-se em princípios físicos intransponíveis do ponto de vista da quebra de segurança.

O protocolo BB84, proposto por Charles Bennett e Gilles Brassard em 1984, é o primeiro protocolo funcional de criptografia quântica. Nele, uma chave secreta é compartilhada entre dois agentes — tradicionalmente chamados de Alice (emissora) e Bob (receptor) — por meio do envio de qubits, que são preparados em bases quânticas não ortogonais. Se um espião, geralmente chamado de Eve, tentar interceptar os qubits, a alteração inevitável no estado das partículas poderá ser detectada posteriormente pelos usuários legítimos.

O BB84 utiliza dois conjuntos de estados base:

- Base retilínea: $|0\rangle$ e $|1\rangle$
- Base diagonal: $|+\rangle$ e $|-\rangle$, onde $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ e $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

Como essas bases são não ortogonais, as medições realizadas em diferentes bases geram incerteza, refletindo diretamente o princípio da superposição e o paradoxo da medição. No protocolo, a aleatoriedade na escolha das bases de Alice e Bob e a subsequente comparação pública das bases (sem revelar os valores) permitem descartar os bits inconfiáveis.

A proposta de utilizar esse protocolo em sala de aula, por meio de um jogo didático, visa contextualizar e concretizar esses conceitos altamente abstratos. Os estudantes, ao simular o envio e recepção de qubits com os macrobits (cartões em formato de círculo/quadrado com cores preta/branca) representando os vetores de estado, vivenciam na prática os efeitos do colapso, da preparação de estados e da não-clonabilidade — todos elementos centrais da mecânica quântica.

Assim, a história da física moderna, da formulação dos postulados quânticos à invenção do BB84, passa a integrar o currículo de forma acessível e lúdica, conectando ciência de ponta

com o cotidiano dos alunos. Esta articulação entre passado e presente, entre teoria e aplicação, é essencial para formar sujeitos críticos e cientificamente alfabetizados.

4. Fundamentação Teórica

4.1 Teorias da Aprendizagem

4.1.1 A importância das teorias de aprendizagem no Ensino de Física

O ensino de Física tem sido historicamente caracterizado pela predominância de metodologias expositivas centradas na transmissão de conteúdos e na resolução mecânica de exercícios. Embora esse modelo tenha contribuído para a consolidação de conhecimentos científicos ao longo do tempo, diversos estudos na área de Ensino de Ciência evidenciam que tal abordagem apresenta limitações quando o objetivo é promover aprendizagens profundas, especialmente em conteúdos de elevada abstração, como aqueles pertencentes à Física Moderna e Contemporânea.

No que tange à Física Moderna e Contemporânea, o ensino de Física enfrenta desafios significativos. Os conceitos são abstratos, contraintuitivos e distantes da vivência cotidiana dos alunos. Para enfrentar essa realidade, torna-se fundamental adotar uma abordagem pedagógica que reconheça o aluno como sujeito ativo do processo de aprendizagem, e não mero receptor de conteúdos prontos.

A Mecânica Quântica constitui um exemplo emblemático dessa dificuldade. Seus conceitos rompem com a experiência cotidiana dos estudantes e exigem a construção de modelos mentais bastante distintos daqueles desenvolvidos a partir da Física Clássica. Assim, ensinar conteúdos como superposição de estados, bases de medição, probabilidade quântica e colapso do vetor de estado requer muito mais do que apresentar definições ou equações matemática, exige a criação de situações didáticas capazes de favorecer a construção gradual de novos significados.

Nesse contexto, as teorias da aprendizagem assumem papel fundamental ao oferecer fundamentos científicos para a elaboração de estratégias pedagógicas coerentes com os processos cognitivos envolvidos na construção do conhecimento. Em vez de compreender o estudante como mero receptor de informações, essas teorias reconhecem a aprendizagem como um processo ativo, social, histórico e culturalmente situado.

Entre as diversas perspectivas existentes na literatura educacional, esta pesquisa fundamenta-se principalmente na teoria histórico-cultural de Lev Vygotsky e na pedagogia crítica de Paulo Freire. A escolha desses referenciais decorre da natureza colaborativa do Produto Educacional desenvolvido, no qual os estudantes interagem continuamente entre si e com o professor durante a resolução das atividades relacionadas ao protocolo BB84.

Ambas as teorias compreendem o conhecimento como resultado das interações humanas e da mediação pedagógica, atribuindo ao professor o papel de organizador das condições necessárias para que o estudante avance em sua compreensão da realidade. Dessa forma, a utilização do macrobit e do jogo didático ultrapassa a dimensão lúdica, constituindo-se como instrumento mediador da aprendizagem.

4.1.2 A teoria histórico-cultural de Lev Vygotsky

Lev Semionovich Vygotsky (1896-1934) desenvolveu uma das mais influentes teorias da aprendizagem do século XX. Diferentemente das perspectivas que compreendiam o desenvolvimento cognitivo como resultado predominantemente biológico, Vygotsky defendeu

que o desenvolvimento intelectual ocorre mediante as interações sociais estabelecidas pelo indivíduo ao longo de sua vida.

Segundo Vygotsky, o ser humano apropria-se da cultura produzida historicamente por meio das relações estabelecidas com outros indivíduos mais experientes. A aprendizagem, portanto, não é um processo individual isolado, mas uma construção social mediada pela linguagem, pelos instrumentos culturais e pelas interações humanas.

Essa perspectiva apresenta profunda relevância para o ensino de Física, pois reconhece que conceitos científicos não são descobertos espontaneamente pelos estudantes. Pelo contrário, precisam ser reconstruídos mediante processos de mediação conduzidos pelo professor e apoiados em atividades colaborativas capazes de favorecer a elaboração de novos significativos.

No contexto desta pesquisa, essa concepção manifesta-se durante todas as etapas do jogo didático baseado no protocolo BB84. À medida que os estudantes discutem estratégias, confrontam hipóteses, justificam escolhas e interpretam resultados, ocorre um processo contínuo de negociação de significados que favorece a compreensão dos conceitos quânticos.

4.1.3 Mediação pedagógica

Um dos conceitos centrais da teoria histórico-cultural é o de mediação. Para Vygotsky, o ser humano não estabelece uma relação direta com o mundo. Essa relação ocorre sempre por meio de elementos mediadores, que podem assumir a forma de instrumentos materiais ou de signos culturais. É justamente essa mediação que diferencia os processos psicológicos humanos dos comportamentos observados em outros animais.

No ambiente escolar, a mediação é desempenhada principalmente pelo professor.

Entretanto, a mediação não se restringe à explicação verbal dos conteúdos. Ela envolve a seleção de problemas, a organização das atividades, a elaboração de perguntas, o acompanhamento das discussões e a utilização de recursos didáticos capazes de favorecer e aprendizagem.

No Produto Educacional desenvolvido nesta dissertação, o macrobit constitui um importante instrumento de mediação. Embora não represente literalmente um qubit, ele permite

aos estudantes manipular representações concretas das diferentes bases de medição utilizadas no protocolo BB84, reduzindo parte da abstração característica da Mecânica Quântica.

Da mesma forma, o jogo assume função mediadora ao organizar situações de interação nas quais os estudantes precisam tomar decisões, argumentar, negociar interpretações e construir coletivamente soluções para os problemas apresentados.

4.1.4 Instrumentos e signos

Outro conceito fundamental na teoria vygotskyana refere-se à distinção entre instrumentos e signos. Os instrumentos são elementos utilizados para transformar o ambiente externo, enquanto os signos atuam sobre os próprios processos mentais no indivíduo, organizando sua atividade psicológica. A linguagem constitui o principal sistema de signos desenvolvido historicamente pela humanidade, permitindo a construção de conceitos, categorias e formas complexas de pensamento. No ensino de Física, modelos, diagramas, representações gráficas, analogias, experimentos e jogos podem funcionar simultaneamente como instrumentos e signos, favorecendo a construção de significados científicos.

Nesse sentido, o macrobit representa um instrumento pedagógico que, associado às discussões realizadas em sala de aula, se transforma também em signo, auxiliando os estudantes na organização de conceitos abstratos relacionados à Mecânica Quântica.

4.1.5 Funções Psicológicas Superiores

Segundo Vygotsky, o desenvolvimento humano é caracterizado pela transformação gradual das funções psicológicas elementares em funções psicológicas superiores.

As funções psicológicas superiores incluem processos como atenção voluntária, memória lógica, pensamento abstrato, planejamento, argumentação e resolução consciente de problemas. Diferentemente das funções elementares, essas capacidades são construídas socialmente mediante processos educativos e culturais.

Ao participar do jogo proposto nesta pesquisa, os alunos são continuamente convidados a formular hipóteses, interpretar informações, comparar estratégias, prever resultados e justificar suas decisões. Essas atividades mobilizam precisamente funções psicológicas

superiores relacionadas ao pensamento científico, favorecendo não apenas a aprendizagem dos conteúdos, mas também o desenvolvimento intelectual dos participantes.

4.1.6 Zona de Desenvolvimento Proximal

Entre as principais contribuições de Lev Vygotsky para a Educação destaca-se o conceito de Zona de Desenvolvimento Proximal (ZDP), considerado um dos pilares da teoria histórico-cultural. Segundo o autor, a aprendizagem não deve ser compreendida apenas como consequência do desenvolvimento cognitivo, mas como um dos principais fatores capazes de promovê-lo.

Vygotsky distingue dois níveis de desenvolvimento do estudante. O primeiro corresponde ao Nível de Desenvolvimento Real, representado pelos conhecimentos, habilidades e competências que o indivíduo já domina e consegue mobilizar de forma autônoma, sem auxílio externo. O segundo corresponde ao Nível de Desenvolvimento Potencial, que engloba tarefas que o estudante ainda não consegue realizar sozinho, mas que se tornam possíveis mediante a orientação de um professor ou a colaboração de colegas mais experientes.

O intervalo existente entre esses dois níveis constitui a Zona de Desenvolvimento Proximal. É justamente nessa região que a aprendizagem ocorre de maneira mais eficiente, pois o estudante é constantemente desafiado a superar seus conhecimentos prévios mediante processos de interação, mediação e colaboração.

No contexto desta pesquisa, a ZDP manifesta-se durante toda a aplicação do Produto Educacional. Inicialmente, os estudantes possuem conhecimentos oriundos da Física Clássica, da Matemática e de experiências cotidianas relacionadas à comunicação digital. Entretanto, ainda não dispõem dos conceitos necessários para compreender a lógica da Mecânica Quântica.

Ao longo da sequência didática, professor organiza situações de aprendizagem nas quais os estudantes são conduzidos, gradativamente, da compreensão de fenômenos clássicos para conceitos próprios da Física Quântica. Esse percurso é realizado por meio de analogias, questionamentos, discussões coletivas, manipulação do macrobit e resolução colaborativa de

problemas, possibilitando que conhecimentos inicialmente inacessíveis passem a integrar o repertório conceitual dos alunos.

Desse modo, o Produto Educacional foi estruturado para atuar precisamente na Zona de Desenvolvimento Proximal dos estudantes, respeitando seus conhecimentos prévios e oferecendo desafios compatíveis com seu nível de desenvolvimento cognitivo.

4.1.7 Nível de Desenvolvimento Real e Nível de Desenvolvimento Potencial

Para compreender adequadamente a Zona de Desenvolvimento Proximal, torna-se necessário distinguir seus dois componentes fundamentais.

O nível de Desenvolvimento Real corresponde às capacidades que o estudante já consolidou. Trata-se dos conhecimentos que podem ser mobilizados sem auxílio externo, representando aquilo que o aluno efetivamente domina no momento da aprendizagem.

No início da aplicação desta pesquisa, verificou-se, por meio do pré-teste, que os estudantes apresentavam domínio relativamente satisfatório de conteúdos como probabilidade e conhecimentos elementares sobre criptografia clássica, embora demonstrassem pouca familiaridade com conceitos específicos da Mecânica Quântica. Esses conhecimentos prévios constituíram o ponto de partida para toda a sequência didática.

Por outro lado, o Nível de Desenvolvimento Potencial refere-se às competências que podem ser desenvolvidas quando o estudante recebe apoio adequado. Nesse caso, a aprendizagem ocorre mediante processos de cooperação entre professor e alunos ou entre os próprios estudantes.

Durante a aplicação do jogo, foi possível observar que muitos conceitos inicialmente considerados complexos passaram a ser compreendidos após sucessivas interações entre os participantes.

A troca de argumentos durante as discussões sobre escolha das bases de medição, compartilhamento de chaves criptográficas e tentativa de interceptação das mensagens constitui exemplo típico de aprendizagem ocorrendo da Zona de Desenvolvimento Proximal.

4.1.8 A internalização como processo de aprendizagem

Outro conceito central da teoria histórico-cultural refere-se ao processo de internalização.

Segundo Vygotsky, todo conhecimento é inicialmente construído no plano social para, posteriormente, tornar-se parte da estrutura cognitiva do indivíduo. Em outras palavras, aquilo que primeiro ocorre entre as pessoas passa, gradualmente, a ocorrer no pensamento do próprio sujeito.

Essa concepção possui grande relevância para o Ensino Médio. Conceitos científicos altamente abstratos dificilmente são apropriados mediante simples exposição oral. Antes de

serem compreendidos individualmente, precisam ser discutidos, manipulados, questionados e reconstruídos coletivamente.

Na proposta desenvolvida nesta pesquisa, o jogo baseado no protocolo BB84 cria sucessivas oportunidades para que os estudantes verbalizem hipóteses, expliquem suas decisões, comparem interpretações e confrontem diferentes estratégias. Esse processo favorece a reconstrução progressiva dos conceitos científicos, permitindo que conhecimentos inicialmente compartilhados coletivamente sejam gradualmente internalizados pelos participantes.

4.1.9 A internalização como processo de aprendizagem

Na teoria histórico-cultural, a linguagem ocupa posição central no desenvolvimento humano.

Para Vygotsky, a linguagem não constitui apenas um meio de comunicação, mas o principal instrumento de organização do pensamento. É por meio dela que os indivíduos atribuem significados ao mundo, elaboram conceitos científicos e desenvolvem formas cada vez mais complexas de raciocínio.

No Ensino de Física, o diálogo entre professor e estudantes representa muito mais do que um mecanismo de transmissão de informações. As discussões realizadas em sala de aula permitem que os alunos reorganizem seus próprios esquemas conceituais, estabeleçam relações entre diferentes conhecimentos e atribuam sentido aos fenômenos estudados.

Durante a aplicação do Produto Educacional, as constantes discussões entre os grupos desempenharam papel fundamental na construção dos conceitos relacionados ao protocolo BB84. Em diversos momentos, observou-se que estudantes inicialmente inseguros passaram a compreender determinados conceitos após ouvir as explicações apresentadas pelos próprios colegas, evidenciando a importância das interações sociais para a aprendizagem científica.

4.1.10 A pedagogia crítica de Paulo Freire

Enquanto Vygotsky enfatiza os processos de mediação e desenvolvimento cognitivo, Paulo Freire direciona sua reflexão para a dimensão social, política e emancipatória da educação.

Freire critica aquilo que denomina educação bancária, caracterizada pela simples transmissão de informações do professor para o estudante, concebido como sujeito passivo do processo educativo. Em oposição a essa perspectiva, propõe uma educação dialógica, problematizadora e libertadora, fundamentada na participação ativa dos estudantes na construção do conhecimento.

Segundo Freire, ensinar não significa transferir conhecimentos prontos, mas criar condições para que os educandos produzam seus próprios saberes por meio do diálogo, da reflexão crítica e da problematização da realidade.

Essa perspectiva apresenta profunda convergência com os objetivos desta pesquisa.

Durante a aplicação do jogo, o professor não fornece imediatamente todas as respostas. Pelo contrário, propõe situações-problema que exigem investigação, argumentação e tomada de

decisões por parte dos estudantes. Dessa forma, o conhecimento deixa de ser apresentado como verdade acabada, passando a ser construído coletivamente durante o desenvolvimento da atividade.

“Ensinar não é transferir conhecimento, mas criar as possibilidades para a sua própria produção ou a sua construção.”

— Paulo Freire, *Pedagogia do Oprimido* (1987)

4.1.11 O diálogo como princípio pedagógico

Um dos conceitos centrais da pedagogia freiriana é o diálogo. Para Paulo Freire, o diálogo representa muito mais do que uma conversa entre professor e estudante. Trata-se de uma relação horizontal baseada no respeito mútuo, na escuta, na problematização e na construção coletiva do conhecimento.

Na presente pesquisa, o diálogo manifesta-se continuamente durante o desenvolvimento do jogo. Os estudantes discutem estratégias, analisam hipóteses, justificam respostas, identificam possíveis erros e reinterpretem conceitos à medida que novas situações surgem durante a atividade.

Esse ambiente dialógico favorece não apenas a aprendizagem dos conteúdos científicos, mas também o desenvolvimento da autonomia intelectual, da capacidade argumentativa e do pensamento crítico.

4.1.12 Aprendizagem Significativa de Ausubel e suas contribuições para o ensino de Mecânica Quântica

A Teoria da Aprendizagem Significativa, proposta por David Paul Ausubel, constitui um dos referenciais mais influentes da psicologia cognitiva aplicada à educação. Em oposição às abordagens baseadas na memorização mecânica, Ausubel (2003) defende que a aprendizagem ocorre de forma significativa quando novas informações conseguem estabelecer relações substantivas e não arbitrárias com conhecimentos prévios, funcionam como conceitos âncora capazes de atribuir significado aos novos conteúdos.

Segundo Ausubel (2003), “o fator isolado mais importante que influencia a aprendizagem é aquilo que o aluno já sabe”. Essa afirmação evidencia a importância de identificar e

considerar os conhecimentos prévios dos estudantes durante o planejamento das atividades didáticas, permitindo que os novos conceitos sejam integrados de maneira organizada e progressiva.

Na perspectiva ausubeliana, a aprendizagem significativa difere da aprendizagem mecânica por promover uma reorganização da estrutura cognitiva do indivíduo. Enquanto a aprendizagem mecânica caracteriza-se pela simples memorização de informações, frequentemente esquecidas em curto prazo, a aprendizagem significativa favorece a compreensão conceitual, a retenção duradoura do conhecimento e a capacidade de aplicar os conceitos em novas situações.

Ausubel também destaca que a aprendizagem significativa depende de três condições fundamentais: a existência de conhecimentos prévios relevantes, a organização lógica e potencialmente significativa do material de ensino e a disposição do estudante para estabelecer relações entre os novos conhecimentos e aqueles já existentes em sua estrutura cognitiva. A ausência de qualquer uma dessas condições tende a dificultar o processo de construção do conhecimento.

Esses princípios apresentam grande relevância para o ensino da Física, especialmente quando se abordam conteúdos de elevada abstração, como aqueles pertencentes à Mecânica Quântica. Diversos estudos apontam que conceitos como superposição de estados e princípio da incerteza representam obstáculos epistemológicos para estudantes da Educação Básica, em razão de seu distanciamento em relação às experiências cotidianas e às concepções desenvolvidas a partir da Física Clássica.

Nesse contexto, torna-se fundamental desenvolver estratégias pedagógicas que estabeleçam pontes entre os conhecimentos já consolidados pelos estudantes e os novos conceitos científicos. A utilização de analogias, modelos didáticos, experimentos investigativos e simulações favorece a construção dessas conexões cognitivas, tornando os conteúdos mais acessíveis e promovendo maior compreensão conceitual.

A proposta didática desenvolvida nesta pesquisa fundamenta-se nesses pressupostos ao utilizar o protocolo BB84 como elemento organizador da aprendizagem. Em vez de apresentar inicialmente os formalismos matemáticos da Mecânica Quântica, a sequência didática parte de uma situação-problema relacionada à segurança da informação, tema presente no cotidiano dos estudantes por meio de aplicativos bancários, redes sociais e sistemas de comunicação digital. A partir dessa contextualização são introduzidos gradualmente conceitos como vetor de estado, estados quânticos, bases de medição e o paradoxo de medição quântica, permitindo

que os alunos estabeleçam relações progressivas entre conhecimentos familiares e os novos conceitos físicos.

Além disso, a sequência didática foi organizada segundo o princípio da diferenciação progressiva, também proposto por Ausubel, no qual conceitos mais gerais são apresentados inicialmente e, posteriormente, desdobrados em conceitos mais específicos e complexos. Paralelamente, buscou-se promover a reconciliação integradora, favorecendo a articulação entre os novos conhecimentos e conteúdos previamente estudados na Física, como Movimento Circular Uniforme e Vetores.

Dessa forma, a Teoria da Aprendizagem Significativa oferece o suporte pedagógico para a organização da proposta de ensino apresentada nesta pesquisa, orientando tanto a elaboração das atividades quanto a interpretação dos resultados obtidos durante sua aplicação. Ao privilegiar a construção gradual do conhecimento, a contextualização dos conteúdos e a valorização dos conhecimentos prévios dos estudantes, a proposta busca favorecer uma aprendizagem mais profunda, duradoura e capaz de aproximar os conceitos da Mecânica Quântica da realidade dos alunos.

4.1.13 Articulação entre Vygotsky, Paulo Freire e o Produto Educacional

A proposta pedagógica desenvolvida neste trabalho fundamenta-se na complementaridade entre os referenciais de Lev Vygotsky e Paulo Freire. Enquanto a teoria histórico-cultural fornece elementos para compreender os processos cognitivos envolvidos na aprendizagem dos conceitos científicos, a pedagogia freireana orienta a organização das práticas educativas a partir do diálogo, da problematização e da participação ativas dos estudantes.

Nesse contexto, o macrobit não é concebido apenas como um recurso lúdico ou ilustrativo. Sua principal função consiste em atuar como instrumento de mediação pedagógica, permitindo que conceitos abstratos da Mecânica Quântica sejam reconstruídos coletivamente por meio das interações estabelecidas entre professor, estudantes e atividade proposta.

O jogo inspirado no protocolo BB84 constitui, portanto, uma estratégia metodológica que integra aspectos cognitivos, sociais e pedagógicos da aprendizagem. Ao longo de sua aplicação, os estudantes deixam de ocupar uma posição passiva diante do conhecimento científico, assumindo um papel de protagonismo na resolução dos desafios apresentados. Essa dinâmica favorece o desenvolvimento da autonomia intelectual, da argumentação científica, da colaboração entre pares e da compreensão conceitual dos princípios fundamentais da criptografia quântica.

4.2 Teorias Quânticas

4.2.1 Introdução conceitual de mecânica quântica

A mecânica quântica constitui uma das teorias fundamentais da física moderna, responsável por descrever o comportamento de sistemas físicos em escalas microscópicas, como átomos, elétrons e fótons. Diferentemente da mecânica clássica, na qual os estados físicos são definidos por variáveis bem determinadas (como posição e momento), a mecânica quântica descreve o estado de um sistema por meio de um vetor de estado pertencente a um espaço vetorial complexo, conhecido como espaço de Hilbert.

Nesse contexto, o estado de um sistema é representado por um vetor $|\psi\rangle$, pertencente a um espaço de Hilbert H , o qual contém toda a informação fisicamente acessível sobre o sistema:

$$|\psi\rangle \in H \quad (1)$$

A estrutura desse espaço permite a definição de um produto interno $\langle\phi|\psi\rangle = 1$, essencial para a interpretação probabilística da teoria. Em especial, a norma do vetor de estado deve satisfazer a condição de normalização:

$$\langle\psi|\psi\rangle = 1 \quad (2)$$

As grandezas físicas observáveis são representadas por operadores lineares hermitianos que atuam sobre os vetores de estado. Se $\hat{A}$ é um operador associado a um observável, então os possíveis resultados de uma medida são dados pelos autovalores da equação:

$$\hat{A}|\psi\rangle = a|\psi\rangle \quad (3)$$

Além disso, o valor esperado de uma grandeza física em um determinado estado é dado por:

$$\langle A \rangle = \langle\psi|\hat{A}|\psi\rangle \quad (4)$$

A evolução temporal de um sistema quântico isolado é governada pela equação de Schrödinger, que estabelece como o vetor de estado varia no tempo:

$$i\hbar \frac{\partial}{\partial t} |\psi(t)\rangle = \hat{H}|\psi(t)\rangle \quad (5)$$

Onde $\hat{H}$ é o operador Hamiltoniano do sistema. Em sua representação na base de posição, essa equação pode ser escrita como:

$$i\hbar \frac{\partial\psi(x,t)}{\partial t} = -\frac{\hbar^2}{2m} \nabla^2\psi(x,t) + V(x)\psi(x,t) \quad (6)$$

Um dos aspectos mais característicos da mecânica quântica é o princípio da superposição.

Um estado quântico pode ser descrito como uma combinação linear de estados base do espaço vetorial de Hilbert. Para um sistema de dois níveis, tem-se:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \quad (7)$$

Com coeficientes complexos α e β , sujeitos à condição de normalização:

$$|\alpha|^2 + |\beta|^2 = 1 \quad (8)$$

No contexto da teoria da medida, a probabilidade de obtenção de um determinado resultado associado a um autovetor $|a\rangle$ é dada por:

$$P(a) = |\langle a|\psi\rangle|^2 \quad (9)$$

Esse postulado introduz um caráter intrinsecamente probabilístico à mecânica quântica, em contraste com a descrição determinística da mecânica clássica.

Essa formulação abstrata da teoria foi consolidada nas primeiras décadas do século XX a partir das contribuições de diversos cientistas, entre os quais se destacam Max Planck, Albert Einstein, Werner Heisenberg e Erwin Schrödinger. O formalismo matemático moderno foi posteriormente sistematizado por autores como Paul Dirac e John von Neumann.

De acordo com o formalismo da teoria, toda grandeza física observável é representada por um operador linear hermitiano. Os possíveis resultados de uma medição correspondem aos autovalores desse operador, enquanto os estados associados a esses valores são denominados autoestados. Assim, a descrição completa de um sistema quântico envolve tanto o vetor de estado quanto os operadores correspondentes às observáveis físicas.

Segundo Paul Dirac em sua formulação clássica da teoria, o estado de um sistema quântico contém toda a informação fisicamente acessível sobre o sistema, e as probabilidades dos resultados experimentais podem ser calculadas a partir da decomposição desse estado na base dos autoestados do observável considerada.

4.2.2 O Princípio da incerteza de Heisenberg

Esse princípio impõe limites à precisão simultânea na determinação de pares de observáveis não comutantes, como posição e momento:

$$\Delta x \cdot \Delta p \geq \frac{\hbar}{2} \quad (10)$$

Esse princípio não decorre de limitações experimentais, mas sim da própria estrutura matemática da teoria, quando o modelo do pacote de ondas é usado para a descrição das partículas quânticas.

4.2.3 O Princípio da Superposição de Autoestados

Esse princípio estabelece que, se um sistema quântico pode estar em dois estados distintos, qualquer combinação linear desses estados também constitui um estado fisicamente possível.

Matematicamente, se $|\psi_1\rangle$ e $|\psi_2\rangle$ são autoestados de um operador associado a um determinada observável, então um estado geral do sistema pode ser escrito como

$$|\psi\rangle = c_1 |\psi_1\rangle + c_2 |\psi_2\rangle \quad (11)$$

onde c_1 e c_2 são coeficientes complexos que determinam as amplitudes de probabilidade associadas a cada estado.

De acordo com a interpretação probabilística da mecânica quântica, formulada por Max Born, o módulo quadrado desses coeficientes (c_1 e c_2) determina a probabilidade de obtenção de cada resultado de medição. Dessa forma, o estado quântico não descreve uma propriedade física definida antes da medição, mas sim um conjunto de possibilidades associadas a probabilidades específicas.

O princípio da superposição é responsável por fenômenos tipicamente quânticos, como interferência e entrelaçamento, e constitui também o fundamento conceitual para a teoria da informação quântica. Como discutido por Michael A. Nielsen e Isaac L. Chuang, a possibilidade de representar estados como superposições de autoestados permite que sistemas quânticos codifiquem informação de maneira qualitativamente diferente dos sistemas clássicos.

Nesse contexto, a unidade fundamental de informação quântica é o qubit, que pode ser representado como uma superposição dos estados básicos $|0\rangle$ e $|1\rangle$. Essa propriedade permite explorar novas formas de processamento e transmissão de informação baseadas nas leis da mecânica quântica.

4.2.4 O Processo de Medição e o Colapso do Vetor de Estado

Outro aspecto fundamental da mecânica quântica refere-se ao papel da medição. Diferentemente da física clássica, na qual a medição revela propriedades previamente existentes do sistema, na mecânica quântica o processo de medição altera o estado do sistema observado.

De acordo com o postulado da medição, quando um observável físico é medido, o resultado obtido corresponde a um dos autovalores do operador associado a essa grandeza. Após a medição, o estado do sistema colapsa para o autoestado correspondente ao valor observado. Assim, se um sistema inicialmente se encontra no estado

$$|\psi\rangle = c_1 |\psi_1\rangle + c_2 |\psi_2\rangle \quad (12)$$

e é realizada uma medição na base formada pelos autoestados $|\psi_1\rangle$ e $|\psi_2\rangle$, o estado do sistema passa a ser um desses autoestados após a medição, com probabilidades dadas por $|c_1|^2$ e $|c_2|^2$.

Esse processo é conhecido como colapso do vetor de estado. Como discutido por John von Neumann, esse postulado representa um dos elementos mais característicos da interpretação padrão da mecânica quântica.

Uma consequência fundamental desse princípio é que medições realizadas em bases diferentes podem produzir resultados incompatíveis. Se um sistema é preparado em um autoestado de um determinado observável e posteriormente medido em relação a outra base, o resultado da medição torna-se probabilístico e o estado do sistema colapsa para um dos autoestados da nova base de medição.

4.2.5 Superposição, Colapso e Segurança na Criptografia Quântica

As propriedades fundamentais da mecânica quântica discutidas anteriormente — superposição de estados e colapso do vetor de estado — desempenham papel central no funcionamento da criptografia quântica.

Um dos protocolos mais importantes nessa área é o BB84 protocol, proposto em 1984 por Charles H. Bennett e Gilles Brassard. Esse protocolo permite a distribuição segura de chaves criptográficas utilizando estados quânticos preparados em diferentes bases de medição.

A segurança do protocolo está diretamente relacionada ao fato de que um estado quântico preparado em uma determinada base pode ser descrito como uma superposição dos autoestados de outra base incompatível. Assim, quando um observador realiza uma medição em uma base diferente daquela utilizada na preparação do estado, o resultado obtido é intrinsecamente probabilístico.

Além disso, o processo de medição provoca o colapso do vetor de estado para um dos autoestados da base utilizada. Caso um terceiro agente tente interceptar a comunicação realizando medições nos estados transmitidos, ele inevitavelmente introduzirá perturbações na sequência de estados enviada, pois sua medição provocará o colapso do estado em uma base possivelmente incompatível com a base de preparação.

Quando os participantes legítimos da comunicação comparam posteriormente as bases utilizadas, essas perturbações manifestam-se na forma de erros detectáveis na sequência de bits compartilhada. Dessa forma, qualquer tentativa de interceptação da comunicação pode ser identificada.

Assim, a segurança do protocolo BB84 não depende de limitações tecnológicas ou computacionais, mas sim de propriedades fundamentais da mecânica quântica, especialmente da relação entre superposição de estados e colapso do vetor de estado durante o processo de medição.

4.3 Segurança da informação

4.3.1 Transmissão de mensagens

Em qualquer contexto, seja ele tecnológico, científico ou cotidiano, a transmissão de mensagens envolve etapas que vão além do simples envio de informações de um emissor para um receptor. Para a compreensão desse processo, um ponto fundamental é distinguir esses conceitos, que são frequentemente confundidos, como codificação e encriptação.

Codificar uma mensagem significa convertê-la em um formato adequado para a transmissão, armazenamento ou processamento. Geralmente, seguindo regras previamente estabelecidas e conhecidas por quem irá recebê-las.

Já a encriptação tem como objetivo ocultar o conteúdo da mensagem, fazendo com que fique inacessível a pessoas não autorizadas, mesmo que essas consigam interceptá-las.

Essa distinção é fundamental, pois enquanto a codificação busca eficiência e compatibilidade, a encriptação prioriza segurança e confidencialidade. Assim sendo, ao longo

desta discussão, será importante considerar não apenas como as mensagens são representadas, mas também quais são as intenções e os mecanismos envolvidos em sua transformação e interpretação.

A transmissão de mensagens é uma etapa fundamental em sistemas de comunicação, atuando na transferência de informação de um emissor para um receptor. A informação pode ser constituída de diversas formas – texto, som, imagem ou dados – e, para ser transmitida de maneira segura, precisa passar por diversas etapas de transformação, garantindo eficiência, integridade total da mensagem, além de confidencialidade do conteúdo enviado.

De maneira geral, a transmissão de mensagens pode ser definida como um fluxo organizado de etapas, que podem ser descritas da seguinte forma:

I. Geração e obtenção da mensagem

O processo se inicia com a criação da mensagem pelo emissor. Essa mensagem é, em sua forma original, compreensível para todas as pessoas e, portanto, não necessariamente adequada para ser transmitida por sistemas digitais.

II. Codificação da mensagem

A mensagem é convertida para uma sequência numérica. Em sistemas digitais, essa conversão ocorre, geralmente, por meio de padrões de codificação – tabelas de caracteres – que associam cada símbolo a um número. Em seguida, esses números são representados em base binária, ou seja, numa sequência de bits (zeros e uns). Essa etapa é fundamental, pois computadores e sistemas digitais operam exclusivamente com sinais binários. Um exemplo de codificação, que será usado mais tarde, é mostrado na primeira coluna da figura 1.

III. Criptografia da informação

Para garantir a segurança da mensagem durante a transmissão é aplicado um processo de criptografia. Nesse contexto, a sequência de bits original é convertida em uma nova sequência, aleatória, utilizando um algoritmo e uma chave de criptografia, representada também como uma sequência binária. Nessa etapa o emissor utiliza a porta XOR para criptografar a informação. O objetivo é garantir que terceiros não sejam capazes de compreender a mensagem, mesmo que tenham acesso aos dados transmitidos.

IV. Compartilhamento da chave criptográfica

Uma das etapas mais críticas de todo o processo é o compartilhamento da chave entre o emissor e o receptor. Essa chave deve ser transmitida por meio seguro, de maneira que apenas o receptor legítimo tenha acesso a ela. Caso a chave seja interceptada, a segurança de todo o sistema é comprometida e a etapa de criptografia não atinge seu objetivo.

V. Transmissão pelo canal de comunicação

A mensagem criptografada é então enviada através de um canal de comunicação, que pode ser físico, como cabos, ou sem fio, como ondas eletromagnéticas. Durante essa etapa, a mensagem pode estar sujeita a ruídos e interferências, o que exige, em sistemas mais complexos, o uso de técnicas adicionais de detecção e correção de erros.

VI. Recepção da mensagem

Nessa etapa o receptor adquire a sequência de bits transmitida. A mensagem, nesse ponto, ainda está criptografada e codificada, sendo necessária a aplicação de processos inversos para recuperar a mensagem original.

VII. Descriptografia

Utilizando a mesma chave (ou uma chave correspondente, dependendo de qual seja o sistema utilizado), o receptor aplica o algoritmo de descriptografia para recuperar a sequência original de bits. É nessa etapa que a porta XOR desempenha um papel fundamental.

A porta XOR é utilizada amplamente em sistemas de criptografia simples devido às suas propriedades. Sua operação básica é mostrada na segunda coluna da figura 1.

Código de dois bits:	Operação XOR:	Leituras de M-bits:	
A = 0 0	$0 + 0 = 0$	 Cor	Branco = "0" Preto = "1"
T = 0 1	$0 + 1 = 1$		
C = 1 0	$1 + 0 = 1$	 Forma	Círculo = "0" Quadrado = "1"
G = 1 1	$1 + 1 = 0$		

Figura 1 - Tabela ASCII-equivalente

- $0 + 0 = 0$
- $1 + 1 = 0$
- $0 + 1 = 1$
- $1 + 0 = 1$

Uma característica fundamental da operação XOR é que ela é reversível, ou seja, quando aplicada duas vezes com a mesma chave é possível a obtenção do original. Desta maneira, se uma mensagem M é criptografada com uma chave C , produzindo $R = M + C$, então a aplicação novamente da operação XOR com a mesma chave irá obter a mensagem original: $M = R + C = (M + C) + C$.

Isso ocorre porque $C + C = 0$, e $M + 0 = M$. Desta maneira, a mesma operação é utilizada tanto para a etapa de criptografia quanto para a de descryptografia, o que torna o processo simples e eficiente.

VIII. Decodificação da mensagem

Após a etapa de descryptografia, a sequência de bits é convertida novamente para a sua forma numérica original e, em seguida, traduzida para símbolos compreensíveis (como caracteres de texto), utilizando o mesmo padrão de codificação aplicado pelo emissor.

IX. Interpretação pelo receptor

Finalmente, o receptor interpreta a mensagem recuperada, completando assim o processo de comunicação.

4.3.2 Macrobit

O macrobit é dispositivo didático em escala macroscópica concebido para simular, de forma acessível, alguns aspectos conceituais da mecânica quântica, especialmente no que diz respeito à representação de estados e ao processo de medida. Se trata, portanto, de um recurso didático e experimental que permite estabelecer analogias com sistemas quânticos, como é o caso do qubit, sem recorrer a fenômenos genuinamente quânticos.

a) Construção física do macrobit

O macrobit é construído como um objeto clássico na forma de um cilindro de seção circular. Sua superfície lateral é pintada de um lado com apenas a face branca visível, enquanto que simetricamente do lado oposto é pintada com apenas a face preta visível. Essa configuração permite que, dependendo da orientação do cilindro, sejam produzidas diferentes “leituras” possíveis, dependendo de qual seja o ponto de vista do observador.

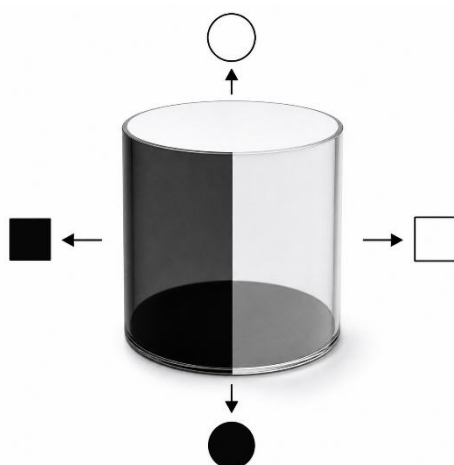


Figura 2 – Macrobit



Figura 3 – cartões representativos dos macrobits

Para permitir uma fácil aplicação do macrobit, são utilizados cartões que representam as quatro possíveis vistas laterais do cilindro. Esses cartões podem ter formato circular ou quadrado, sendo que cada um de seus lados tem uma cor: branca ou preta. Assim sendo, ao

manipular esses cartões – o que seria análogo ao observar o cilindro sob diferentes perspectivas – é obtido um sistema que apresenta resultados distintos conforme a base de medição, estabelecendo um paralelo com a escolha de base em sistemas quânticos.

b) O ato de “medir” o macrobit

A medição do macrobit corresponde a escolher uma determinada base de medição, atribuindo um valor binário conforme a escolha do critério de observação ou base na linguagem da mecânica quântica. Um conjunto de atribuições possíveis é aquele mostrado na terceira coluna da figura 1. Dependendo da escolha, o resultado obtido será uma das duas possibilidades (na escolha de forma: quadrado ou círculo; na escolha de cor: preto ou branco). Essa dependência da medida em relação ao contexto reproduz a ideia de escolha de base em sistemas quânticos.

Assim sendo, o macrobit simula a “escolha quântica” não por meio de indeterminação intrínseca, mas por meio da ambiguidade clássica. O observador, ao selecionar uma forma de observação, determina qual aspecto do sistema será usado para sua medição. Ao fazer tal escolha, o resultado passa a ser apenas um, o que corresponde ao colapso do vetor de estado. A limitação clássica aqui se encontra no fato do macrobit não pode inviabilizar a observação da outra base de medição, no sentido de que medir usando o critério cor não altera a forma do macrobit, algo que ocorreria num sistema quântico real.

c) Interpretação e linguagem: paralelo com a mecânica quântica

A descrição do macrobit é frequentemente feita utilizando a linguagem formal da mecânica quântica, em especial a noção de vetor de estado, que é um conceito mais abrangente e fundamental, mas com associações mais simples em relação ao próprio macrobit. Diferentemente da função de onda, o vetor de estado oferece uma representação mais direta e abstrata do sistema, além de estabelecer uma conexão imediata com o conceito de qubit, que também é descrito nesse formalismo.

Com isso, o macrobit pode ser associado a um vetor de estado que representa uma combinação de possibilidades de observação. Contudo, é importante destacar que essa “combinação” não corresponde a uma superposição quântica real, mas apenas a uma ambiguidade clássica controlada. Ou seja, o sistema não está simultaneamente em vários estados físicos possíveis, está apenas representando resultados distintos a depender da forma como será observado.

Essa ambiguidade, ilustrada na figura 4 (em combinação com a terceira coluna da figura 1), tenta reproduzir, em nível conceitual, uma das características mais marcantes da mecânica quântica: a dependência do resultado da medida em relação à base escolhida. Assim, o macrobit permite simular, até certo ponto, a ideia de superposição de estados, mesmo que não envolva qualquer fenômeno quântico.

A pergunta da figura 4 é impossível de ser respondida antes de se determinar a base de medição escolhida. Já a figura 5 não apresenta qualquer ambiguidade, uma vez que a escolha da base de medição não resultará em um bit diferente, essa limitação mostra o caráter clássico do macrobit.

“0” or “1” ?



Figura 4 – Ambiguidade da medida

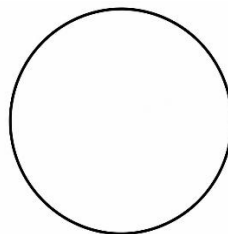


Figura 5 – Não tem ambiguidade

d) Ausência do princípio da incerteza

Um ponto importante na análise do macrobit é a ausência do princípio da incerteza. Em sistemas quânticos genuínos, certos pares de observáveis não podem ser determinados simultaneamente com precisão indefinida. Para o caso do macrobit, por se tratar de um objeto clássico, todas as suas propriedades estão bem definidas a todo momento. A

limitação da observação decorre exclusivamente da configuração do experimento e da perspectiva adotada, e não de uma restrição fundamental da natureza.

Com isso, qualquer indeterminação associada ao macrobit é epistemológica, e não ontológica.

e) O macrobit não é um sistema quântico

Embora utilize a linguagem e simule certos comportamentos da mecânica quântica, é essencial enfatizar que o macrobit não é um sistema quântico. Ele não apresenta superposição real, emaranhamento ou colapso do vetor de estado. Todas as suas propriedades são determinadas por sua construção física e pelas regras clássicas que governam sua utilização.

Seu valor reside, portanto, na capacidade de reproduzir, de maneira clara e intuitiva, aspectos formais da teoria quântica, permitindo a exploração de conceitos complexos com ferramentas clássicas e acessíveis.

f) Uso do vetor de estado

A escolha por descrever o macrobit em termos de vetor de estado, em vez da função de onda, se deve à sua maior abrangência e sua aplicabilidade em sistemas discretos. Além disso, essa escolha facilita a conexão conceitual com o qubit, cuja descrição padrão também se dá nesse formalismo. O vetor de estado permite representar diretamente as probabilidades associadas às diferentes bases de observação, mesmo em um sistema clássico como o macrobit.

g) Simulação da medida quântica com sistemas clássicos

A utilização do macrobit possibilita simular o processo da medida quântica utilizando dispositivos inteiramente clássicos. Por meio do uso dos cartões e da escolha de diferentes bases de medição, é possível reproduzir experimentalmente comportamentos análogos aos observados em sistemas quânticos reais.

Essa característica torna o macrobit uma ferramenta muito valiosa tanto para fins didáticos quanto para o desenvolvimento de protocolos inspirados na mecânica quântica.

h) Papel do macrobit na transmissão segura de mensagens

O macrobit desempenha um papel extremamente relevante na etapa de compartilhamento da chave de criptografia. Os protocolos inspirados na criptografia quântica,

como a distribuição de chaves baseada na escolha aleatória de bases, podem ser simulados através dos macrobits.

A ambiguidade inerente ao sistema garante que terceiros, ao tentar fazer a leitura da chave, não consigam obter a informação completa sem revelar sua presença. Embora essa “perturbação” não seja de natureza quântica, ela pode ser modelada de forma a evidenciar inconsistências detectáveis entre emissor e receptor, desde que sejam deliberadamente provocadas durante a transmissão.

Desta maneira, o macrobit permite o uso, em um ambiente clássico, dos princípios fundamentais de comunicação segura e um dos pilares da criptografia quântica que é a impossibilidade de observação sem interferência.

Em resumo, o macrobit constitui um elo conceitual entre sistemas clássicos e quânticos, permitindo a simulação de aspectos fundamentais da mecânica quântica e sua aplicação em problemas como a transmissão segura de informações. Apesar de suas limitações, sua simplicidade e versatilidade o tornam uma ferramenta poderosa para a compreensão e experimentação de ideias avançadas.

4.3.3 O uso do macrobit na criptografia do jogo

No contexto da transmissão de mensagens, o macrobit tem um papel fundamental e mais crítico em todo o processo, que é o compartilhamento da chave de criptografia.

Ao ser descrito na linguagem de vetor de estado, o macrobit – que é uma analogia ao qubit – permite representar diferentes possibilidades de resultado associadas a distintas bases de medição. Contudo, diferentemente de um sistema quântico real, essa multiplicidade não decorre de uma superposição física, mas de uma ambiguidade estrutural do objeto. Assim, ao escolher uma base de medida (cor ou forma), o observador define qual propriedade será usada na medição do macrobit, enquanto a outra permanece inacessível e indeterminada no contexto da observação.

Essa característica é fundamental para a simulação do processo de medida quântica. A ação de “medir” o macrobit corresponde à escolha prévia de um critério de observação, o que determina o resultado obtido. Caso diferentes observadores utilizem bases de medição diferentes, os resultados não serão, em sua totalidade, similares. Essa dependência da medida

em relação à escolha da base de medição simula, em nível conceitual, a lógica do mecanismo pelo qual a segurança é moldada.

Desta maneira, o macrobit permite simular, com recursos clássicos, a ideia de que a tentativa de obtenção de informação por terceiros, sem conhecimento da base de medição correta, introduz inconsistências detectáveis. Apesar de não haver um princípio físico análogo ao princípio da incerteza quântica, a limitação de informação surge da própria estrutura do sistema e das regras adotadas.

Em resumo, o macrobit desempenha um papel fundamental no jogo como mediador entre a teoria e a prática, entre o objeto clássico e a analogia quântica. Essa capacidade de simular conceitos abstratos da mecânica quântica (como na escolha da base de medição, na medida e na representação por vetor de estado) em uma experiência prática, que é o jogo, mostra a sua extrema importância.

5. Metodologia

Esta pesquisa está fundamentada como um estudo de natureza aplicada, com abordagem predominantemente qualitativa e complementada por elementos quantitativos, tendo como objetivo investigar as potencialidades da utilização do protocolo BB84 como recurso didático para o ensino de conceitos da Mecânica Quântica no Ensino Médio.

A opção pela abordagem qualitativa está apoiada na necessidade de compreender os processos de aprendizagem, as interpretações dos estudantes e as contribuições pedagógicas proporcionadas pela sequência didática desenvolvida. Conforme encontramos na literatura, pesquisas qualitativas permitem analisar fenômenos educacionais em seu contexto natural, considerando as interações entre pesquisador, participantes e ambiente de aprendizagem.

Os elementos quantitativos foram empregados para complementar a análise qualitativa por meio da comparação dos resultados obtidos nos instrumentos avaliativos aplicados antes e após a intervenção pedagógica. Essa combinação metodológica possibilitou uma compreensão mais abrangente do impacto da proposta educacional, caracterizando um estudo de método misto com predominância qualitativa.

5.1 Tipo de pesquisa

Quanto aos objetivos, esta investigação enquadra-se como uma pesquisa exploratória e descritiva.

A pesquisa exploratória justifica-se pelo fato de existirem poucas propostas didáticas voltadas ao ensino da criptografia quântica e do protocolo BB84 na Educação Básica brasileira. Assim, buscou-se ampliar a compreensão acerca das possibilidades pedagógicas desse conteúdo, identificando dificuldades, potencialidades e estratégias de ensino.

Ao mesmo tempo, caracteriza-se como pesquisa descritiva por analisar as interações dos estudantes durante a aplicação da sequência didática, descrevendo o comportamento da turma, as dificuldades conceituais observadas e as aprendizagens evidenciadas ao longo das atividades.

Sob a perspectiva dos procedimentos técnicos, trata-se de uma pesquisa de intervenção pedagógica, uma vez que o pesquisador elaborou, aplicou e avaliou uma sequência didática especificamente desenvolvida para abordar conceitos fundamentais da Mecânica Quântica por meio do protocolo BB84.

5.2 Contexto da pesquisa

A pesquisa foi desenvolvida em duas escolas particulares do estado do Rio de Janeiro, envolvendo estudantes regularmente matriculados na 2ª série do Ensino Médio. Uma das turmas ficou com o papel de turma de controle, sendo exposta ao modelo tradicional de apresentação do conteúdo, enquanto a outra turma ficou sujeita a aplicação do Produto Educacional.

A escolha dessa etapa da Educação Básica ocorreu devido ao fato de os estudantes já possuírem conhecimentos prévios sobre Mecânica Clássica, Ondulatória e Óptica, além de Probabilidade. Conteúdos considerados essenciais para compreender as propriedades físicas envolvidas na simulação da criptografia quântica.

As atividades foram realizadas durante as aulas regulares da disciplina de Física, respeitando o planejamento escolar sem prejuízo ao currículo previsto pela Base Nacional Comum Curricular (BNCC).

O número de participantes correspondeu aos estudantes presentes nas turmas durante o período de aplicação da sequência didática, sendo garantidos todos os princípios éticos relacionados ao anonimato, à confidencialidade dos dados e à participação voluntária.

5.3 Instrumentos de coleta de dados

Para a obtenção dos dados foram utilizados diferentes instrumentos, permitindo a triangulação das informações coletadas.

Inicialmente foi aplicado um questionário diagnóstico com o objetivo de identificar os conhecimentos prévios dos estudantes acerca de conceitos relacionados à Mecânica Clássica, à Mecânica Quântica, criptografia, comunicação segura, Física Moderna e Probabilidade.

Posteriormente, durante o desenvolvimento da atividade lúdica, foram realizados registros sistemáticos das observações em sala de aula, contemplando aspectos como participação dos estudantes, dúvidas recorrentes, interação entre os grupos e estratégias utilizadas para resolução das atividades propostas.

Foram realizados registros sistemáticos das observações em sala de aula da turma que ficou submetida a exposição tradicional do conteúdo, contemplando aspectos como participação dos estudantes, dúvidas recorrentes e interação entre os alunos e o professor.

Ao final da intervenção foi aplicado um questionário avaliativo contendo questões objetivas destinadas a verificar a evolução conceitual dos estudantes e suas percepções sobre a proposta didática.

Além dos questionários, foram analisadas as produções escritas dos alunos, registros das atividades práticas e respostas apresentadas durante as simulações do protocolo BB84.

Essa diversidade de instrumentos permitiu confrontar diferentes evidências de aprendizagem, aumentando a confiabilidade dos resultados obtidos, apesar das limitações que a própria pesquisa possui, como um baixo espaço amostral (apenas duas turmas) e pequena diversidade dos alunos (por serem duas escolas particulares do mesmo estado e de cidades próximas – Rio de Janeiro e Niterói).

5.4 Desenvolvimento da sequência didática

A sequência didática foi estruturada com base nos princípios da aprendizagem significativa proposto por Ausubel (2003) e organizada em etapas progressivas, buscando estabelecer conexões entre conhecimentos previamente adquiridos e os novos conceitos introduzidos.

A primeira etapa consistiu na problematização da necessidade de segurança na transmissão de informações, utilizando exemplos cotidianos envolvendo comunicação digital, aplicativos bancários, redes sociais e sistemas criptográficos tradicionais.

Na segunda etapa foram introduzidos os fundamentos físicos necessários para compreender o protocolo BB84, incluindo vetor de estado, estados quânticos, superposição, princípio da medida e impossibilidade de clonagem de estados quânticos.

Em seguida, os estudantes que pertenciam a turma selecionada para a aplicação do Produto Educacional participaram de atividades práticas simulando o funcionamento do protocolo BB84. Durante essas atividades representaram os papéis de emissor e receptor, realizando codificação, encriptamento, medição e comparação das bases utilizadas.

Na etapa final, foram promovidas discussões coletivas acerca das limitações da criptografia clássica, das vantagens oferecidas pela distribuição quântica de chaves e das aplicações atuais da informação quântica em sistemas reais de comunicação.

5.5 Procedimentos de análise dos dados

Os dados qualitativos foram submetidos a três etapas: pré-análise, exploração do material e tratamento dos resultados.

Na pré-análise realizou-se a organização dos registros obtidos durante a aplicação da sequência didática.

Na etapa de exploração foram identificadas categorias relacionadas à compreensão dos conceitos físicos, dificuldades apresentadas pelos estudantes, desenvolvimento do raciocínio científico e percepção acerca da utilização do protocolo BB84 como ferramenta de aprendizagem.

Posteriormente, procedeu-se à interpretação dos resultados, estabelecendo relações entre as categorias emergentes, a literatura especializada e os objetivos da pesquisa.

Os dados quantitativos foram organizados por meio de estatísticas descritiva, utilizando frequências absolutas, frequências relativas, médias e comparação entre os desempenhos obtidos antes e após a intervenção pedagógica.

A integração entre as análises qualitativas e quantitativas permitiu construir uma interpretação mais consistente dos efeitos da sequência didática sobre a aprendizagem dos estudantes.

5.6 Aspectos éticos

Esta pesquisa observou os princípios éticos estabelecidos para pesquisas envolvendo estudantes de Ensino Médio, garantindo o anonimato dos participantes e a confidencialidade das informações coletadas.

Os estudantes participaram voluntariamente das atividades, sendo esclarecidos acerca dos objetivos da investigação e da utilização exclusivamente acadêmica dos dados obtidos.

Todas as informações apresentadas nos resultados foram tratadas de forma agregada, impossibilitando a identificação individual dos participantes.

5.7 Proposta didática

Proposta didática: o jogo do encriptamento quântico BB84.

Para tornar os conceitos de criptografia quântica acessíveis e significativos ao público do Ensino Médio, foi desenvolvido um jogo educativo que simula, de forma lúdica e concreta, o protocolo BB84, um dos pilares da criptografia quântica.

O objetivo principal do jogo é permitir que os estudantes vivenciem o processo de encriptamento e desencriptamento de uma mensagem de forma segura, utilizando conceitos centrais da mecânica quântica como superposição, preparação de estados, colapso do vetor de estado, e o paradoxo da medição quântica.

5.7.1 Descrição do jogo

Objetivo do jogo:

Simular o envio de uma mensagem de 3 letras codificadas (a partir de uma sequência genômica A T C G) por meio de qubits, utilizando duas bases diferentes de medição (relação com o protocolo BB84), em um cenário com possibilidade de interceptação.

A escolha pela sequência genômica como alfabeto se justifica pela necessidade de compatibilizar a representação com a estrutura operacional do sistema proposto, especialmente no que se refere à utilização de palavras binárias de 6 bits. A adoção de um alfabeto convencional muito extenso implicaria em um crescimento significativo da quantidade de macrobits necessários para representar cada símbolo, tornando o sistema computacionalmente mais complexo e operacionalmente inviável. Nesse contexto, a sequência genômica apresenta uma alternativa eficiente, pois permite a construção de um conjunto simbólico reduzido, porém suficientemente diverso para codificação e manipulação de informação.

O macrobit é um objeto clássico que fará o papel de atuar na visualização da aprendizagem dos conceitos da mecânica quântica, especialmente para ilustrar o comportamento de um qubit. Ele se apresenta sob a forma de um cilindro reto de seção circular pintado de modo que para cada face branca do cilindro haverá uma complementar preta. Por praticidade, durante a prática pedagógica, são usados cartões que imitam cada uma das 4 vistas laterais possíveis de um macrobit. Eles podem ser tanto circular quanto quadrado, e possui duas cores: branca de um lado e preta do outro. O objetivo principal do macrobit é representar a medição de um qubit, simulando o resultado do colapso do vetor de estado, conceito fundamental da física quântica. Embora o macrobit seja um modelo clássico e, portanto, tenha limitações em comparação ao seu representante quântico, ele pode ser uma excelente ferramenta pedagógica para explicar as complexidades do comportamento quântico. Para isso, a escolha do critério de observação na qual será feita a medida, antes dela ser realizada, assume um papel fundamental para que seja possível essa simulação, já que é isso que garante a segurança da transmissão. Isso ocorre porque, ao interagir com o macrobit, os

alunos conseguem perceber, de maneira simplificada, os paradoxos e as implicações do mundo quântico.

Apesar de ser um objeto clássico, o macrobit tem um papel de analogia didática para o entendimento de algumas características do comportamento de um qubit, especialmente quando os estudantes aumentam o simbolismo associado às diferentes bases de leitura. Nesse modelo, as propriedades “forma” e “cor” não representam diretamente os valores medidos, mas sim bases distintas de observação. Independente de qual base seja escolhida, o resultado obtido será sempre binário (0 ou 1), mas o significado desse resultado dependerá do contexto da medida realizada. Essa característica introduz uma ambiguidade semelhante à existente na língua portuguesa em palavras como “sabia”, cuja interpretação pode variar conforme o uso do acento agudo (“sábua”, “sabia” ou “sabiá”). Analogamente, em sistemas quânticos, o resultado de uma medida só adquire significado físico completo quando a base de medição é conhecida. Com isso, o macrobit permite ilustrar, de forma intuitiva, a dependência contextual da medida quântica e a relação entre base de observação, superposição de estados e colapso do sistema após a medição.

Materiais necessários:

- Macrobits.
- Pasta transparente com régua suporte para os macrobits.
- Fichas e tabelas de correspondência (base usada $\leftrightarrow$ bit lido).
- Um “roteiro do jogo” com regras e etapas para guiar a atividade.
- Quadro branco ou tela de projeção para discussão coletiva.

Papéis dos jogadores:

- Emissor: codifica uma mensagem de 3 letras (cada letra será transformada em um conjunto de 6 bits - 2 bits por caractere), escolhe aleatoriamente um critério de observação para cada bit e prepara o macrobit.
- Receptor: faz a leitura dos bits recebidos escolhendo também uma base de medição aleatória para cada bit.

1) Mensagem (escolha qualquer combinação de três caracteres entre A T C G):

T	G	C
---	---	---

2) Codifique a mensagem em uma sequência binária de seis caracteres usando a primeira coluna da tabela A:

0	1	1	1	1	0
---	---	---	---	---	---

3) Monte um conjunto de 25 M-bits e fixe-os no suporte.

4) Construa uma chave com seu parceiro para criptografar a mensagem codificada em 2.

- Selecione e anote na 2ª coluna da tabela B, 15 bases para ler a sequência de M-bits.
- Escreva a representação binária correspondente na 3ª coluna da tabela B, após a 3ª coluna da tabela A.
- Aguarde os anúncios do receptor para preencher a 4ª coluna da tabela B da outra página marcando S sempre que ele escolher a mesma base que você.

5) Chave – pegue os seis primeiros resultados da 3ª coluna da tabela B se a 4ª coluna estiver marcada por S:

1	1	0	1	1	1
---	---	---	---	---	---

6) Use as sequências binárias que representam a mensagem codificada em (2) e a chave de criptografia em (5) como entradas para a operação XOR seguindo a segunda coluna da tabela A e escreva os resultados na linha designada para a mensagem criptografada.

Mensagem codificada (2)	0	1	1	1	1	0
Chave de criptografia (5)	1	1	0	1	1	1
Mensagem criptografada	1	0	1	0	0	1

7) Anuncie os bits da mensagem criptografada ao Receptor

TGC

Figura 6 – Tabela do Emissor: O aluno escolheu a sequência TGC como mensagem e a codificou conforme a tabela de codificação na sequência 01 11 10 e criptografou com a sequência 10 10 01 usando a chave de criptografia 11 01 11

3) Chave – pegue os seis primeiros resultados da 3ª coluna da tabela B se a 4ª coluna estiver marcada por S:

1	1	0	1	1	1
---	---	---	---	---	---

4) Peça ao Emissor a sequência que representa a mensagem criptografada:

1	0	1	0	0	1
---	---	---	---	---	---

5) Use as sequências binárias que representam a chave de criptografia em (3) e a mensagem criptografada em (4) como entradas para a operação XOR seguindo a segunda coluna da tabela A e escreva os resultados na linha designada para a mensagem descryptografada.

Chave de criptografia (3)	1	1	0	1	1	1
Mensagem criptografada (2)	1	0	1	0	0	1
Mensagem descryptografada	0	1	1	1	1	0

6) Decodifique a mensagem decifrada usando a 1ª coluna da tabela A:

T	G	C
---	---	---

Figura 7 – Tabela do Receptor: O aluno usou a chave de criptografia 11 01 11 e a mensagem criptografada 10 10 01 para conseguir a mensagem descryptografada 01 11 10

Etapas do jogo:

I. Codificação da mensagem pelo Emissor:

- Alice escolhe 3 letras, a partir de uma base genômica, e converte cada uma em um trio de bits binários (utilizando a tabela ASCII-equivalente).
- Para cada bit, ela escolhe aleatoriamente uma base de preparação (base forma ou cor).
- Cada par (bit, base) gera um macrobit que será “enviado” ao Receptor.

II. Medição pelo Receptor:

- Para cada macrobit recebido, Receptor escolhe aleatoriamente uma base de medição.
- Se sua base for igual à de Emissor, ele obtém o bit corretamente. Essa etapa é o que simula a preparação de estados na mecânica quântica. Caso a escolha da base não igual à do Emissor, ele terá 50% de chance de obter o valor errado.

III. Comparação pública das bases:

- Emissor e Receptor compartilham suas bases publicamente (não os bits).
- Mantêm apenas os bits nas posições em que as bases coincidiram (essa é a chave segura compartilhada).

IV. Descriptografia da mensagem:

- Usando a chave final, Receptor tenta reconstruir a mensagem original de Emissor.
- Os alunos refletem sobre os erros, perdas e sobre a segurança do processo.

[illegible]

Figura 8 - Lista do receptor em folha A3 com a pasta com os macrobits obtidos

5.7.2 Integração com os conceitos da teoria quântica

Durante o jogo, o professor poderá, em diferentes momentos, introduzir os conceitos físicos fundamentais, como:

- Superposição: as bases possíveis maneiras de se fazer uma medida.
- Colapso do vetor de estado: ao medir, Receptor define o estado — o qubit “colapsa”.
- Paradoxo da medição: mesmo sem interceptação, bases incompatíveis geram incerteza.
- Preparo de estados: cada bit preparado por Emissor corresponde a um estado quântico específico.

Esses momentos serão trabalhados como “paradas reflexivas” com os alunos, em que eles são convidados a discutir e registrar o que perceberam, como uma espécie de “diário quântico de bordo”.

Vinculação com os referenciais pedagógicos

- Freire: o jogo promove o diálogo, a escuta e o protagonismo dos estudantes.
- Vygotsky: a mediação do professor e dos pares, bem como o uso de ferramentas simbólicas, favorece a aprendizagem na zona de desenvolvimento proximal.
- Ausubel (em apoio): conceitos complexos são apresentados de forma significativa, partindo do concreto para o abstrato.

5.7.3 Produto educacional

O produto resultante desta proposta será um roteiro completo do jogo BB84, contendo:

- Instruções passo a passo para professores.
- Materiais didáticos (cartões, tabelas, modelos de fichas).
- Sugestões de perguntas problematizadoras.
- Testes pré e pós aplicação do jogo.

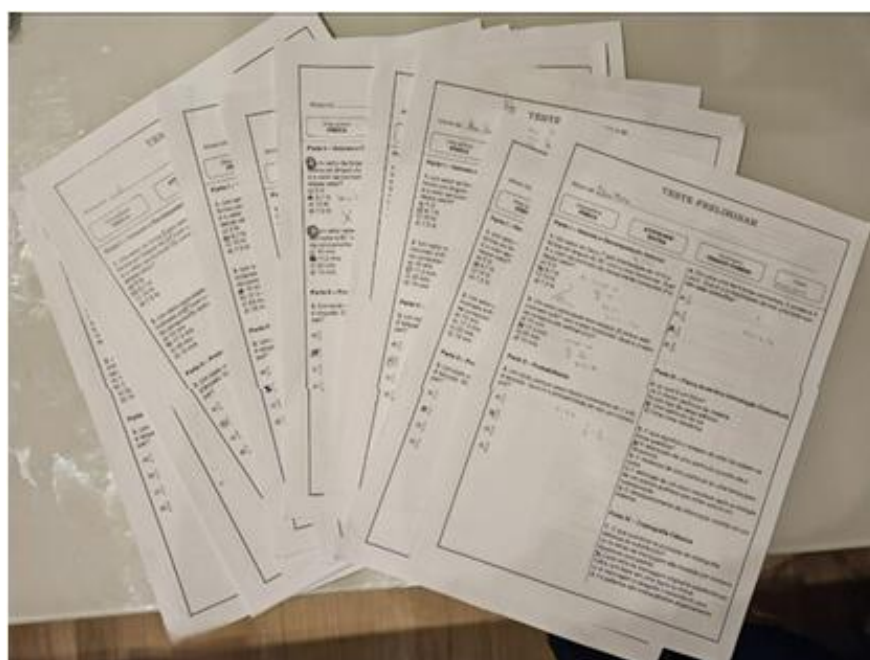


Figura 9 - Teste preliminar realizado pela turma A

6. Avaliação

Objetivo da avaliação

A avaliação nesta proposta cumpre dupla função: verificar a eficácia pedagógica do jogo baseado no protocolo BB84 como ferramenta de ensino de conceitos de física quântica e segurança da informação, e avaliar a participação, compreensão e motivação dos alunos frente ao conteúdo. Mais do que mensurar desempenho, busca-se compreender como os alunos constroem sentido para os fenômenos abordados por meio da experiência lúdica e cooperativa.

Metodologia de avaliação aplicada

Foi utilizado um modelo comparativo onde duas turmas de 2ª série do Ensino Médio de dois colégios particulares foram submetidas a dois testes, um pré-teste e um pós-teste.

Etapas da aplicação

I. Diagnóstico inicial (pré-teste):

- Aplicação de um breve questionário com questões objetivas sobre:
 - Conhecimentos prévios de vetores.
 - Conhecimentos prévios de probabilidade.
 - Conhecimentos prévios de movimento circular.
 - Noções sobre criptografia e segurança digital.

II. Aplicação diferenciada do conteúdo:

- Turma A (experimental): participação no jogo BB84 com mediação ativa do professor e discussão coletiva dos conceitos quânticos.
- Turma B (controle): exposição tradicional do conteúdo, por meio de aula expositiva com quadro e explicação teórica.

III. Questionário pós-jogo (pós-teste):

- Realização de um segundo questionário com os mesmos temas e nível das questões do diagnóstico inicial.
- Um questionário oral sobre o que foi aprendido e o que esse conhecimento pode trazer de ganho no futuro.

IV. Registro observacional:

- Durante a atividade com o jogo, foi feito um registro de campo, com anotações sobre:
 - Nível de engajamento dos alunos.
 - Participação espontânea nas discussões.
 - Clareza nas regras e aplicações dessas no jogo.

V. Critérios de avaliação:

- Foram utilizados indicadores qualitativos com os seguintes critérios:
 - Compreensão conceitual: domínio das ideias de superposição, colapso, preparação de estados e criptografia.
 - Relação símbolo-significado: capacidade de interpretar as fichas/qubits do jogo como representações físicas de estados quânticos.
 - Trabalho colaborativo: disposição para o diálogo, respeito às ideias do outro e resolução conjunta de tarefas.
 - Motivação e interesse: observação de falas espontâneas, engajamento voluntário e relatos sobre aplicações da física no cotidiano.

Expectativas de aprendizagem

Com base nos referenciais de Freire, Vygotsky e Ausubel, espera-se que os alunos da turma experimental:

- Desenvolvam um interesse mais significativo por física moderna, associando-a a contextos atuais e socialmente relevantes (segurança da informação, computação quântica).
- Acessem conceitos complexos de forma significativa, partindo de uma experiência concreta e simbólica (o jogo) para depois construírem os conceitos formais.
- Se reconheçam como sujeitos ativos do processo de aprendizagem, atribuindo sentido ao conteúdo estudado.
- Apresentem melhor desempenho cognitivo e atitudinal em relação aos estudantes da turma controle.

Validação e análise dos dados

Os dados coletados foram analisados com uma abordagem qualitativa e quantitativa, priorizando:

- A evolução da média dos alunos (pré-teste vs. pós-teste).
- A comparação entre as turmas (jogo vs. aula tradicional).
- Os relatos sobre o nível de compreensão e significado atribuído ao conteúdo.
- A consistência entre comportamento observável e aprendizagem declarada.

A avaliação, portanto, não se limitou a medir acertos em provas, mas buscou compreender como o jogo transformou o modo como o estudante se relaciona com a física e com a ideia de ciência como algo vivo, dinâmico e presente em sua realidade.

7. Aplicação do produto

7.1. Dia da dinâmica

A turma A foi reunida e dividida em grupos de dois alunos. Como a turma era composta por 21 alunos, um dos alunos fez dupla com o professor-instrutor.

Foi feita uma breve discussão sobre a importância da segurança digital. O quão fundamental era a proteção das mensagens que são trocadas entre eles através de aplicativos de mensagem, assim como da segurança da proteção de senhas de e-mail, computadores e celulares.

Após essa introdução, os alunos foram convidados a participar de uma dinâmica na qual um aluno escreveria uma senha, e esta deveria ser passada a sua dupla. Para evitar interceptações, essa mensagem seria passada através de um código que só poderia ser entendido pela sua dupla.

A recepção dos alunos foi muito calorosa e entusiasmada. Ao decorrer dos primeiros minutos da introdução da dinâmica, foi necessário acalmar a turma para poder passar as instruções de maneira que todos pudessem compreender e serem capazes de se orientarem a partir das informações contidas nas tabelas que seriam distribuídas. Essa parte da aula levou entre 15 e 20 minutos, desde a discussão sobre a importância da segurança digital até serem passadas as instruções da dinâmica.

Em seguida, cada dupla definiu quem seria o emissor e quem seria o receptor. O aluno que atuou como emissor ficou responsável por começar a dinâmica ao escolher a mensagem de 3 letras e sortear os macrobits. Na sequência, foi entregue ao aluno que atuou como receptor a folha A3 com os 20 macrobits escolhidos.

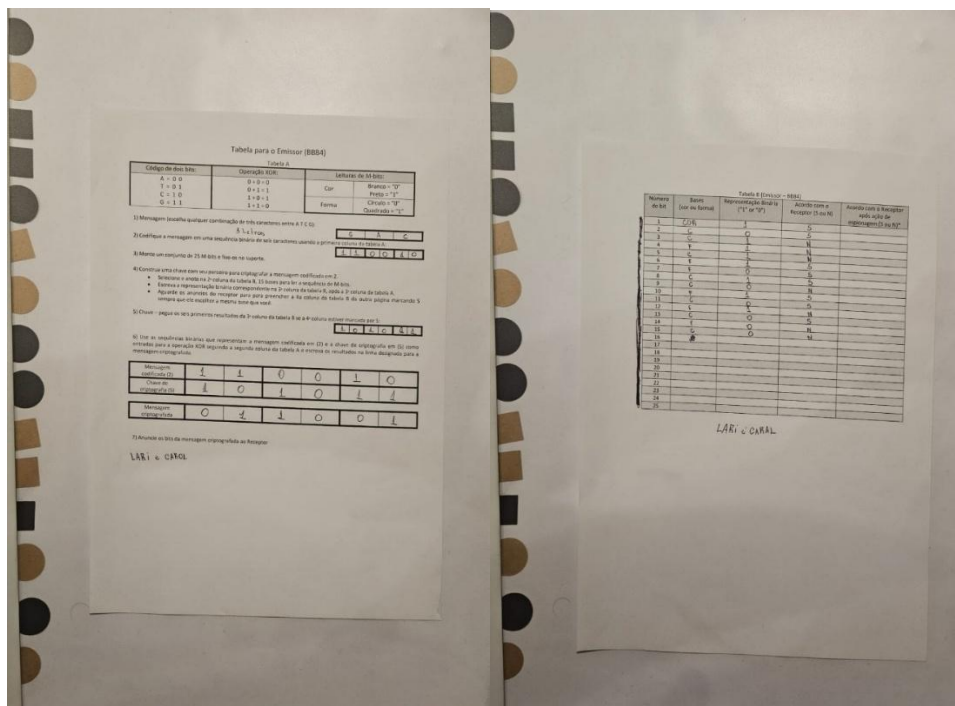


Figura 10 - Folhas do emissor

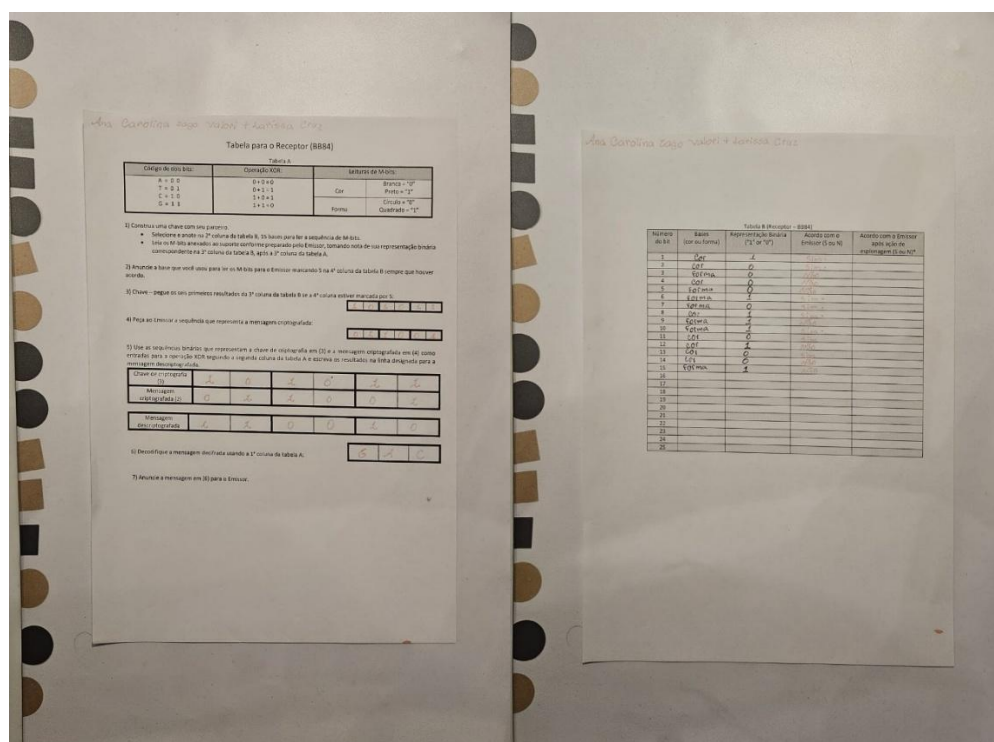


Figura 11 - Folhas do receptor

Propositalmente, não foi feita uma demonstração do jogo completo antes dos alunos começarem a dinâmica. Dessa forma, os alunos foram induzidos a trocarem informações entre as duplas e se orientando através das informações das tabelas para conseguirem seguir nas etapas da dinâmica. Alguns alunos, e duplas, acabaram se perdendo em algum momento, mas todos foram capazes de seguir com a ajuda dos demais e da leitura das tabelas. A atuação do professor-instrutor após o início da dinâmica foi a mínima possível.

Todas as duplas conseguiram obter a mensagem correta. A dinâmica do produto levou entre 20 e 25 minutos até ser completada por todos os alunos.

A obtenção das mensagens corretas e a animação com essa dinâmica geraram debates sobre o funcionamento da mecânica quântica em comparação a mecânica clássica, vista por eles como a “Física que a gente conhece”. Apesar de ser um assunto extremamente novo para eles, foi possível notar uma construção, e o grande interesse, na fundamentação da lógica que emerge da mecânica quântica. Essa inquietação, e curiosidade, dos alunos fez o produto alcançar, nesta etapa, o que se propunha com esse produto, construir uma lógica na dinâmica gerada pelos fundamentos da mecânica quântica, além de dar novos significados, agora numa abordagem quântica.

Ao término da dinâmica, o, aparente, sucesso da aula gerou o início de um debate sobre temas secundários que derivam das aplicações do vasto poderio da mecânica quântica, no que diz respeito a computação, como segurança digital e a importância da utilização de códigos. Os alunos levantaram temas como: O que é criptografar? É 100% seguro trocar mensagens? O quão difícil é decodificar uma senha? Como funciona as mensagens criptografadas do Whatsapp?

O debate não era planejado anteriormente, mas acabou durando entre 5 e 10 minutos. A troca com os alunos acabou sendo mais superficial e utilizada para instigar a curiosidade e

deixar um certo grau de animação para a aula que viria na semana seguinte abordando o tema, mas de uma forma mais tradicional expondo o assunto no quadro.

7.2 Análise da compatibilidade das bases de medida

Um dos pontos mais importantes do jogo é a etapa de comparação das bases de medida que foram escolhidas para cada macrobit que foi selecionado. A leitura correta da mensagem só poderá ser feita se essa etapa for bem sucedida.

Com uma compatibilidade esperada de 50% e uma mensagem de 3 letras, e sei bits, a quantidade mínima probabilística para se trabalhar é com 12 macrobits. Entretanto, essa quantidade não seria a ideal, uma vez que ficaria a mercê de flutuações que podem ocorrer em um espaço amostral tão pequeno. Para contornar esse problema, foram utilizados, inicialmente 15 macrobits. Contudo, caso fosse necessária uma quantidade maior de macrobits para a compatibilidade, a tabela foi preparada para até 25 macrobits, além do uso da folha A3 que permitia esse número de escolhas a serem sorteadas e anexadas.

Com a quantidade utilizada de 15 macrobits o percentual necessário para obtenção de 6 resultados compatíveis seria de 40%. Um valor com uma margem melhor para se trabalhar, mesmo que ainda num espaço amostral pequeno. Porém, o uso de 15 ao invés de 25 macrobits, tornou a dinâmica muito mais rápida e interessante aos alunos, que geralmente perdem o interesse com facilidade em atividades mais longas e repetitivas.

Os materiais das 11 duplas com suas respectivas medidas e compatibilidades foram analisadas e se encontram na tabela a seguir.

Dupla	Compatibilidade	Percentual
1	8/15	53,3%
2	10/15	66,7%
3	9/15	60%
4	13/15	86,7%
5	8/15	53,3%
6	7/15	46,7%
7	9/15	60%
8	11/15	73,3%
9	7/15	46,7%
10	6/15	40%
11	9/15	60%

Tabela A – Compatibilidade na escolha de bases

Podemos perceber, como mostrado acima, que em um dos casos as 6 compatibilidades necessárias ocorreram no limite, um risco já previsto devido a baixa quantidade de medidas, mas, mesmo assim, foram obtidas de forma satisfatória.

Das 11 duplas, 8 delas obtiveram compatibilidades entre 6 e 9, ou seja, entre os percentuais de 40 e 60%. As outras 3 duplas que obtiveram resultados diferentes desse percentual acabaram tendo acertos acima do esperado, o que acabou sendo um bom resultado, apesar de discrepante.

Ao analisarmos todas as duplas, com suas 165 escolhas de base, podemos notar um percentual de compatibilidade de 58,8%.

7.3 Dia da aula tradicional

As aulas foram agendadas para os dois tempos intermediários do dia, 3º e 4º tempos, para que não fosse trabalhado em nenhum horário muito próximo da entrada e nem da saída, dessa forma foi possível contar com a presença de todos os alunos das duas turmas.

As aulas seguiram a mesma ordem e os mesmos assuntos abordados, sem existir nenhum tipo de diferenciação entre turma A e turma B.

A aula teve início com o contraste da mecânica quântica com a física clássica. A primeira pergunta a ser respondida foi “um objeto pode estar em dois lugares ao mesmo tempo?”. Apesar do estado de superposição existir antes da medida, a pergunta serviu como ponto de partida para a ideia de superposição. Escrevi o estado de um qubit no quadro:

$$|\psi\rangle = \alpha |0\rangle + \beta |1\rangle$$

Os alunos da turma B estranharam quase que imediatamente, enquanto que os alunos da turma A rapidamente me indagaram sobre o macrobit trabalhado na dinâmica de aula.

Continuei a aula mostrando que o sistema estava “nos dois” estados (superposição) e que, apesar do desconforto gerado, a lógica clássica não se aplicava a teoria quântica. Isso já gerou em ambas as turmas curiosidade, mesmo que essa curiosidade nos alunos da turma A estivessem envoltas de correlações criadas com o jogo.

Em sequência, apresentei o colapso do vetor de estado. Usei uma moeda como analogia, algo bem comum. Apesar de não ser perfeita, funciona bem para o desejado. O importante era chegar na lógica central: medir não é algo passivo, a medição interfere na própria medida. Era fácil prever que os alunos logo me indagariam com a clássica pergunta: “Então, o simples fato de olhar o experimento, faz o resultado ser alterado?”. Esse tipo de pergunta é muito relevante, pois mostra que os alunos estão conectados a aula e que estão tentando criar explicações para que seja a uma lógica palpável para eles.

É importante salientar que a medição não interfere na medida no caso da moeda. E só ocorre no uso do macrobit por conta da redundância, ou ambiguidade, no que diz respeito à representação binárias das leituras.

Com isso, introduzi as bases de medição. Nessa parte, a diferença da aula da turma A para a turma B chegou ao seu ápice. A formalização matemática foi assustadora para ambas as turmas no geral, algo que eu rapidamente correlacionei com algo mais visual: setas e direções diferentes dependendo de como o observador as vê. Dessa forma, foi possível que os alunos aceitassem com mais tranquilidade o que viria a ser escrito no quadro:

$$|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}, |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

Nesse momento, os alunos da turma A rapidamente foram capazes de correlacionar esta parte da aula com as escolhas das bases (“forma” ou “cor”) do jogo, gerando uma satisfação muito grande em todos por entender, pelo menos em estágios iniciais, o propósito real do jogo.

Já os alunos da turma B não tiveram nenhuma fonte de comparação, tendo em vista que a aula era a única ferramenta didática utilizada para a exposição do conteúdo. Ainda assim, foram capazes de acompanhar a explicação, mesmo que com um pouco mais de discussão e de analogias.

Foi necessário sair do macro, e clássico, para chegar à conclusão necessária. Mostrei a eles que se um sistema está numa mistura de $|0\rangle$ e $|1\rangle$, quando ela é medida, será obtido um resultado apenas. Portanto, a simbologia $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ representa o estado antes de haver a medição. Após a medição: $|0\rangle$ ou $|1\rangle$ (colapso do vetor de estado). Com isso, muitos alunos acabaram indagando o porquê de isso acontecer, pergunta muito natural e, também, muito desejada. Expliquei que, apesar de não sabermos exatamente o porquê, sabemos que acontece e, graças a isso, somos capazes de prever os resultados com muita precisão. Continuei mostrando que o importante era que antes da medição o sistema possui várias possibilidades e que, após a medição apenas uma permaneceria. Sugeri então que os alunos pensassem no seguinte experimento mental: Eu tenho um estado equilibrado, ou seja, 50% $|0\rangle$ e 50% $|1\rangle$. Se eu fizer a medição desse sistema equilibrado várias vezes espero obter um resultado de metade e metade. Porém, a medição individual só me dá apenas um resultado, o 50% só aparece quando o experimento é repetido várias vezes. Com essa ideia, desenhei duas bases no quadro e mostrei que se eu medir na base “certa”, obterei o valor esperado, mas caso eu faça a medição na base “errada” o resultado passa a ser aleatório. Então, temos três fatos importantes:

1. O sistema pode estar em superposição.
2. Medir faz o estado colapsar para um vetor de estado.
3. E o resultado depende da base escolhida.

Com toda essa preparação feita, cheguei ao gancho planejado. Questionei os alunos: “Se medir muda o sistema, o que acontece quando alguém tenta medir sem que você saiba?” Na hora foi possível perceber a inquietude e a animação das turmas com a conclusão que já esperavam, antes mesmo que eu concluísse: “Seria então possível detectar espionagem na mecânica quântica, tornando esse método mais seguro.”

Aproveitei a animação para explicar o protocolo BB84. A turma A acabou recebendo as explicações com mais facilidade e com mais entusiasmo por já ter participado do jogo, enquanto que a turma B demonstrou entendimento com a explicação, mas pedindo para que pudessem fazer uma dinâmica com o jogo.

Por fim, os alunos, em sua maioria, foram capazes de construir uma fundamentação teoria quântica que lhes permitiu entender, ou aceitar sem muitos incômodos, o protocolo BB84 com certa naturalidade. Mesmo que a matemática não fosse tão familiar, a lógica por detrás dela acabava sendo o ponto de apoio deles.

8. Resultados

8.1. Aplicação do pré-teste

O comportamento das duas turmas durante a aplicação do pré-teste foi bem similar. Os alunos aceitaram bem a proposta de um teste livre, sem graduação de nota, para que fosse estabelecido o conhecimento prévio da turma. Foi informado a eles, nesse primeiro momento, que o teste serviria para a preparação de uma aula posterior sobre temas importantes academicamente, como vetores, probabilidade e movimento circular uniforme, além de temas mais atuais como criptografia clássica, criptografia quântica e segurança digital.

O teste possuía 3 questões de vetores, 2 questões de probabilidade, 2 questões de movimento circular uniforme e 4 questões de conceitos de criptografia e segurança digital, além de uma redação.

O desejado não era a análise puramente quantitativa, mas usar o teste como uma ferramenta eficiente para fazer com que os alunos tenham recente na memória assuntos que assumem um papel de grande importância na interpretação e na construção da lógica quântica fundamentada também em conhecimentos clássicos previamente consolidados e lembrados.

O teste preliminar, assim como o pós-produto, se encontra no apêndice 1.

8.1.1 Resultados do pré-teste

Os resultados serão apresentados nas tabelas a seguir onde serão mostrados a quantidade de alunos que acertaram cada quantidade de questões (de zero até o número máximo daquele assunto) e o percentual da turma a que corresponde essa quantidade de alunos.

Turma A (experimental)	Turma B (controle)
21 alunos	21 alunos

Questões de vetores

Acertos	Turma A (alunos; %)	Turma B (alunos; %)
0	5; 23,8%	4; 19,0%
1	10; 47,6%	12; 57,1%
2	6; 28,6%	5; 23,8%
3	0; 0%	0; 0%

Questões de probabilidade

Acertos	Turma A (alunos; %)	Turma B (alunos; %)
0	0; 0%	0; 0%
1	0; 0%	2; 9,5%
2	21; 100%	19; 90,5%

Questões de movimento circular uniforme

Acertos	Turma A (alunos; %)	Turma B (alunos; %)
0	10; 47,6%	6; 28,6%
1	4; 19,0%	11; 52,4%
2	7; 33,3%	4; 19,0%

Questões de criptografia e segurança digital

Acertos	Turma A (alunos; %)	Turma B (alunos; %)
0	6; 28,6%	2; 9,5%
1	4; 19,0%	11; 52,4%
2	4; 19,0%	4; 19,0%
3	4; 19,0%	4; 19,0%
4	3; 14,3%	0; 0%

Resultado geral do teste

Acertos (%acerto)	Turma A (alunos; %)	Turma B (alunos; %)
0-3 (0%-27,3%)	4; 19,0%	3; 14,3%
4-6 (36,4%-54,5%)	10; 47,6%	13; 61,9%
7-9 (63,6%-81,8%)	6; 28,6%	5; 23,8%
10-11 (90,9%-100%)	1; 4,7%	0; 0%

8.1.2 Análise dos resultados

As turmas trabalhadas foram de poucos alunos, 21 alunos, o que favoreceu a organização da turma e a passagem clara de informações a respeito do teste. Por outro lado, o reduzido número de alunos poderia gerar discrepâncias consideráveis nos resultados. Apesar disso, os valores obtidos foram bem similares nas duas turmas, com poucas flutuações significativas, o que corroborou com a premissa de que as turmas estavam niveladas no início do processo.

a) Questões de vetores

Aproximadamente, 20% dos alunos de ambas as turmas obtiveram aproveitamento baixo, entre 0%-32% de acerto das questões; 80% dos alunos de ambas as turmas obtiveram

aproveitamento mediano de 33%-66% de acerto dessas questões; nenhum aluno de ambas as turmas errou todas as questões.

Os resultados apresentam duas turmas de proficiência similar em vetores, o que convergiu com a premissa de que as turmas não só estavam niveladas, como também apresentavam embasamento teórico suficiente para terem a capacidade de fazer associações e interpretações do produto com os conceitos desejados, uma vez que interpretações vetoriais assumem um papel importante na mecânica quântica.

b) Questões de probabilidade

Enquanto a turma A obteve 100% dos alunos acertando ambas as questões de probabilidade, a turma B obteve quase 90% de nota máxima e 10% dos alunos com um acerto.

Os resultados apresentam duas turmas de proficiência similar em probabilidade.

c) Questões de movimento circular uniforme

A turma A obteve quase 48% da turma com nenhum acerto, já a turma B esse valor foi de quase 29%. Na situação de um acerto, a turma A aparece com 19%, enquanto a turma B com quase 53%. Acerto nas duas questões foi visto em 33% da turma A e 19% da turma B.

Os resultados das questões de movimento circular foram bem mais divergentes entre as turmas, porém se analisarmos o total de questões acertadas por turma, esses valores foram de 18 acertos em 42 possíveis na turma A (42,9% de acerto) e de 19 acertos em 42 possíveis na turma B (45,2% de acerto).

Possivelmente, se o teste tivesse apresentado mais questões de movimento circular uniforme (MCU), os resultados obtidos poderiam acabar convergindo para valores mais próximos, contudo o objetivo do teste não era uma análise específica e aprofundada da proficiência em MCU, mas uma análise mais superficial e comparativa das duas turmas.

Do ponto de vista geral das turmas, a proficiência em MCU é similar nas duas turmas.

d) Questões de criptografia e segurança digital

A turma A obteve uma distribuição mais uniforme das notas, com 19% acertando 1 questão, 19% acertando 2 questões e 19% acertando 3 questões. 28,6% não acertaram nenhuma questão e 14,3% acertaram todas as questões. Já a turma B não teve nenhum aluno acertando todas as questões, porém obteve quase 52% da turma acertando uma questão, 19% acertando duas questões e 19% acertando 3 questões.

Se analisarmos o resultado a partir dos acertos totais por turma, obteríamos 36 acertos em 84 possíveis na turma A (42,9% de acerto) e de 31 acertos em 84 possíveis na turma B (36,9% de acerto).

Do ponto de vista geral das turmas, elas apresentam um conhecimento similar sobre os assuntos de criptografia e segurança digital.

e) Resultado geral do pré-teste

Da análise quantitativa, as turmas obtiveram resultados gerais muito similares. Na faixa de acerto entre 0% e 27,3% as duas turmas tiveram entre 14% e 19% dos alunos. Na faixa de acerto entre 36% e 55% as duas turmas tiveram entre 48% e 62%. Na faixa de acerto entre 63,6% e 81,8% as duas turmas tiveram entre 23% e 29%. Já na faixa de acerto entre 90,9% e 100% as duas turmas tiveram entre 0% e 5%.

Da análise qualitativa, o pré-teste alcançou o seu objetivo no que se refere a preparação dos alunos em reviver conceitos fundamentais, como vetores e MCU, para que fosse possível mais adiante estarem preparados, e de mente fresca e ativa, para serem capazes de fazer as analogias necessárias para o entendimento do qubit e das correlações entre a mecânica clássica e a mecânica quântica.

Dessa forma, as duas turmas apresentam proficiências similares nas áreas investigadas, revisitaram os conteúdos fundamentais e estavam aptas a continuar para a próxima etapa.

8.2. Aplicação do pós-teste

A aplicação do pós-teste se deu uma semana após a aplicação do produto na turma A e da aula tradicional na turma B. As duas turmas se comportaram de forma similar durante a aplicação, sem grandes dúvidas nos enunciados e apresentando um certo grau de entusiasmo na

elaboração. É bom enfatizar que os testes não geraram nenhum tipo de bonificação e, boa parte da aceitação e acolhimento, se deu pela introdução de um assunto novo, visto por eles como “moderno”. Além disso, a existência de uma nova dinâmica acaba mexendo com o interesse dos alunos.

8.2.1 Resultados do pós-teste

Turma A (experimental)	Turma B (controle)
21 alunos	21 alunos

Questões de vetores

Acertos	Turma A (alunos; %)	Turma B (alunos; %)
0	2; 9,5%	2; 9,5%
1	7; 33,3%	9; 42,9%
2	12; 57,2%	10; 47,6%

Questões de probabilidade

Acertos	Turma A (alunos; %)	Turma B (alunos; %)
0	0; 0%	0; 0%
1	4; 19%	6; 28,6%
2	17; 81%	15; 71,4%

Conceitos de mecânica quântica

Acertos	Turma A (alunos; %)	Turma B (alunos; %)
0	3; 14,3%	3; 14,3%
1	6; 28,6%	11; 52,4%
2	12; 57,1%	7; 33,3%

Questões de criptografia

Acertos	Turma A (alunos; %)	Turma B (alunos; %)
0	2; 9,5%	3; 14,3%
1	3; 14,3%	4; 19,1%
2	3; 14,3%	7; 33,3%
3	8; 38,1%	5; 23,8%
4	5; 23,8%	2; 9,5%

Resultado geral do teste

Acertos	Turma A (alunos; %)	Turma B (alunos; %)
0-3 (0%-30,0%)	0; 0%	0; 0%
4-5 (40%-50%)	4; 19,0%	7; 33,3%
6-7 (60%-70%)	8; 38,1%	10; 47,6%
8-10 (80%-100%)	9; 42,9%	4; 19,1%

8.2.2 Análise dos resultados

A aplicação do pós-teste se deu em circunstâncias semelhantes a aplicação do pré-teste. As turmas já tinham uma experiência anterior e o quantitativo reduzido de alunos permitiu uma organização mais rápida. Em poucos minutos os alunos já estavam em suas cadeiras preparados para fazer a atividade.

O pós-teste apresentou 2 questões de vetores, 2 questões de probabilidade, 2 questões conceituais sobre mecânica quântica e 4 questões de criptografia.

O teste teve como objetivo avaliar se os alunos se sentiriam mais confortáveis em responder questões sobre mecânica quântica e criptografia, bem como analisar como se comportariam no pós-teste.

a) Questões de vetores

As duas turmas obtiveram 2 alunos com zero acertos, o que representa menos de 10% de cada turma. A turma A obteve 33,3% da turma com 1 acerto e 57,2% com 2 acertos. Já a turma B obteve 42,9% da turma com 1 acerto e 47,6% com 2 acertos.

As duas turmas apresentaram uma melhora considerável nas questões de vetores, com a turma A se destacando mais que a turma B.

Essa melhora pode ter como origem a aplicação do produto para a turma A e a aula tradicional para a turma B. Contudo, parte dessa melhora pode ter sido obtida com a aplicação do teste preliminar que fez o papel de trazer à lembrança dos alunos esse conteúdo, que possivelmente estava adormecido.

b) Questões de probabilidade

As duas turmas não tiveram nenhum aluno com zero acertos. A turma A obteve 19% da turma com 1 acerto e 81% com 2 acertos. Já a turma B obteve 28,6% da turma com 1 acerto e 71,4% com 2 acertos.

Ambas as turmas mantiveram o alto índice de acerto nas questões de probabilidade, como já havia ocorrido no pré-teste. O que demonstra que, para o nível trabalhado nas questões, as duas turmas estavam tranquilas e dominando o conteúdo.

c) Conceitos de mecânica quântica

Tanto a turma A como a turma B tiveram 14,3% dos alunos com 0 acertos. A turma A obteve 28,6% dos alunos com 1 acerto e 57,1% dos alunos com 2 acertos. Já a turma B obteve 52,4% dos alunos com 1 acerto e 33,3% com 2 acertos.

As duas turmas apresentaram um bom rendimento com destaque para a turma A que obteve mais da metade dos alunos com acertos em ambas as questões. Já a turma B apresentou mais da metade da turma com acerto em pelo menos uma das duas questões.

d) Questões de criptografia e segurança digital

A turma A obteve 9,5% dos alunos com nenhum acerto, 14,3% com 1 acerto, 14,3% com 2 acertos, 38,1% com 3 acertos e 23,8% com acerto nas 4 questões. Já a turma B obteve 14,3% dos alunos com nenhum acerto, 19,1% com 1 acerto, 33,3% com 2 acertos, 23,8% com 3 acertos e 9,5% com acerto nas 4 questões.

A turma A obteve mais de 60% da turma com 75% ou mais de acerto, enquanto a turma B obteve mais de 30% da turma com o mesmo aproveitamento. Quando analisamos o aproveitamento em 50% ou mais de acertos, a turma A obteve mais de 76% da turma, enquanto a turma B obteve mais de 66% da turma.

O resultado das duas turmas pode ser considerado muito satisfatório, não só pelo resultado quantitativo apresentado, mas principalmente pela postura leve com que os alunos trataram a ideia de fazer um teste com questões que abordavam criptografia, algo que antes era visto como um assunto desconhecido e, agora, como um assunto dito por muitos como “interessante”.

e) Resultado geral do pós-teste

As duas turmas apresentaram um aproveitamento muito bom no pós-teste. A turma A apresentou mais de 80% dos alunos com acertos de 60% ou mais, sendo que quase 43% dos alunos obtiveram 80% ou mais de acertos. Já a turma B apresentou mais de 66% dos alunos com acertos de 60% ou mais, sendo que quase 20% dos alunos conseguiram 80% ou mais de acertos.

Do ponto de vista quantitativo a turma A obteve no pré-teste um pouco mais de 33% dos alunos turma com aproveitamento de mais de 60% das questões, já no pós-teste esse aproveitamento foi para mais de 80% dos alunos. Já nos aproveitamentos abaixo de 30% o resultado saiu de 19% dos alunos no pré-teste para 0% dos alunos no pós-teste.

A turma B por sua vez obteve no pré-teste um pouco mais de 23% dos alunos da turma com aproveitamento maior que 60% das questões, já no pós-teste esse aproveitamento foi para mais de 66% dos alunos. Já nos aproveitamentos abaixo de 30% o resultado saiu de um pouco mais de 14% dos alunos no pré-teste para 0% dos alunos no pós-teste.

Do ponto de vista qualitativo, pôde-se notar na fala dos alunos que estavam mais confiantes e mais a vontade com o teste, bem como com a possibilidade de serem avaliados em novos temas como os relacionados a mecânica quântica e criptografia.

f) Análise de um dos testes

Foram selecionados testes de um aluno da turma A que obteve um rendimento abaixo da turma com recurso de análise para investigar se após a aplicação do produto este aluno apresentaria melhoras significativas no conhecimento dos fundamentos básicos da mecânica quântica e, em segunda análise, se de forma indireta o jogo poderia auxiliar na melhora dos conteúdos escolares regulares, como vetores, probabilidade e MCU.

TESTE PRELIMINAR

Aluno (a): XXXXXXXXXX 02/00 2/11

Disciplina: FÍSICA	ATIVIDADE EXTRA	Professor: THIAGO CABRAL	Data:
------------------------------	---------------------------	------------------------------------	-------

Parte I – Vetores e Decomposição Vetorial

1. Um vetor de força F tem intensidade de 10 N e forma um ângulo de 30° com o eixo horizontal. Qual é o valor aproximado da projeção horizontal (F_x) desse vetor?

☒ a) 5 N
☐ b) 8,7 N
☐ c) 10 N
☐ d) 7,5 N

2. A base α é composta por dois vetores unitários, A e B , perpendiculares entre si. O vetor $\vec{A}$ aponta para o leste, enquanto o vetor $\vec{B}$ aponta para o norte. Considerando o vetor $\vec{R} = \vec{A} + \vec{B}$, assinale a alternativa correta:

☒ a) A intensidade de $\vec{R}$ vale 1 e sua direção forma um ângulo de 45° com a direção leste.
☐ b) A intensidade de $\vec{R}$ vale 2 e sua direção forma um ângulo de 90° com a direção norte.
☐ c) A intensidade de $\vec{R}$ vale $\sqrt{2}$ e sua direção forma um ângulo de 45° com a direção leste.
☐ d) A intensidade de $\vec{R}$ vale $\sqrt{2}$ e sua direção forma um ângulo de 0° com a direção leste.

3. Seja agora uma nova base β composta pelos vetores unitários $\vec{A}'$ e $\vec{B}'$, obtidos ao girar a base original α (formada por $\vec{A}$ e $\vec{B}$) de 45° no sentido anti-horário em relação ao plano horizontal. Admita o vetor $\vec{R}$, que possui projeções (1,1) na base original α , da questão anterior.

Com base nessas informações, assinale a alternativa correta sobre as projeções do vetor $\vec{R}$ na base β :

☒ a) As projeções de $\vec{R}$ permanecem iguais: (1,1), pois a rotação da base não altera as projeções.
☐ b) As projeções de $\vec{R}$ na nova base são (1,0), indicando que ele aponta apenas na direção de $\vec{A}'$.
☐ c) As projeções de $\vec{R}$ na nova base são (0, $\sqrt{2}$), indicando que ele aponta apenas na direção de $\vec{B}'$.
☒ d) As projeções de $\vec{R}$ na nova base são ($\sqrt{2}/2$, $\sqrt{2}/2$), pois o vetor continua com módulo 1 e é igualmente projetado nas direções $\vec{A}'$ e $\vec{B}'$.

Parte II – Probabilidade

4. Um dado comum (seis faces numeradas de 1 a 6) é lançado. Qual é a probabilidade de sair um número par?

☒ a) $\frac{1}{6}$
☐ b) $\frac{2}{3}$
☐ c) $\frac{1}{2}$
☐ d) $\frac{3}{4}$

5. Em um jogo de cartas, Thiago explica que, ao retirar uma carta de um baralho especial com apenas cartas vermelhas, a probabilidade de sair uma carta vermelha é igual a 1.

Com base nessa informação, é correto afirmar que:

☒ a) Uma carta vermelha pode nunca ser sorteada.
☒ b) A ocorrência de sair uma carta vermelha é certa.
☐ c) Nada garante que uma carta vermelha será sorteada.
☐ d) As chances de sair uma carta vermelha são de 50%.

Parte III – Movimento Circular Uniforme

6. Um ciclista percorre uma pista circular de raio constante com velocidade escalar constante. Sobre esse movimento, é correto afirmar que:

☒ a) A velocidade vetorial do ciclista não muda, pois sua velocidade escalar é constante.
☐ b) A aceleração do ciclista é nula, já que ele está em velocidade constante.
☐ c) O movimento do ciclista é retilíneo uniforme, pois ele não muda de direção.
☐ d) A velocidade escalar do ciclista é constante, mas sua velocidade vetorial muda o tempo todo.

ENUNCIADO PARA AS QUESTÕES 8 e 9

A figura abaixo apresenta um gráfico com uma circunferência de raio 1 e centro na origem (0,0).

Esse gráfico representa a cor resultante emitida por um LED devido a combinação dos brilhos de duas componentes: vermelho (eixo y) e verde (eixo x). A partir disso, podem ser feitas as afirmações:

- Nos pontos (0,1) e (0,-1) o LED apresentará a cor vermelha com brilho máximo (e brilho verde nulo).
- Nos pontos (1,0) e (-1,0) o LED apresentará a cor verde com brilho máximo (e brilho vermelho nulo).
- Em todos os pontos da circunferência, o LED irá emitir uma combinação entre a luz verde e a luz vermelha. Quando a intensidade de ambas as cores for a mesma, a LED assume a cor amarela.

8. Qual das coordenadas a seguir apresentará o LED quando assume a cor amarela?

☒ a) $(\frac{\sqrt{2}}{2}, \frac{\sqrt{2}}{2})$
☐ b) $(\sqrt{2}, \sqrt{2})$
☐ c) (0,1)
☐ d) (1,1)

9. O LED é fotografado em momentos aleatórios fornecendo x imagens, onde x é um número muito grande. Nessa situação podemos concluir que o que aparecerá mais vezes nas fotografias é o:

☒ a) LED vermelho.
☐ b) LED amarelo.
☐ c) LED verde.
☒ d) LED apagado.

10. Admita que o eixo xy da base α seja rotacionado em 45° no sentido anti-horário para dar origem a uma nova base β , de eixos $x'y'$. Nesta nova base β , a cor amarela corresponde a quais coordenadas?

☒ a) (0,1)
☐ b) (1,0)
☒ c) ($\sqrt{2}$, 0)
☐ d) (0, $\sqrt{2}$)

11. Um método comum para determinar se um tipo de tecido é ou não original, é o uso de um tipo especial de tinta reagente. Essa tinta é invisível quando aplicada, mas quando em contato com o tecido ela assume uma coloração amarela por alguns instantes, depois assume uma coloração verde ou vermelha, dependendo do tipo de material. Após isso, uma reação química ocorre, tornando a tinta apenas água e incolor, não manchando assim o tecido.

Esse teste só pode ser feito uma única vez, já que a primeira reação química altera permanentemente a natureza molecular do tecido.

Qual das afirmações a seguir está de acordo com a característica desse tipo de teste?

☒ a) É possível aplicar o teste novamente para revelar uma nova cor.
☐ b) A cor só é conhecida no momento da aplicação, após essa reação, o estado do tecido se altera de forma irreversível.
☐ c) Após o teste é possível retornar o tecido para o estado inicial pré-teste.
☐ d) É possível saber o resultado do teste antes mesmo de aplicar a tinta.

DISCURSIVA

12. Imagine que você e seu melhor amigo têm um código secreto pra conversar sem que ninguém mais entenda. Isso é mais ou menos o que a criptografia faz na internet?

Agora, pense e responda:

Por que você acha que a criptografia é importante quando a gente usa redes sociais, faz compras online ou envia mensagens? Você conhece alguma brincadeira ou jogo que envolva a criptografia?

É importante para ter privacidade e segurança. Cuidar da rede e um bom jogo com criptografia.

Figuras 12 e 13 – Páginas 1 e 2 do teste preliminar

O aluno em questão obteve no teste preliminar 0 acertos em vetores, 1 acerto em probabilidade, 0 acertos em MCU e 0 acertos em questões conceituais de roupage de

mecânica quântica. Já no teste pós-produto obteve 2 acertos em vetores, 2 acertos em probabilidade, 5 acertos em questões conceituais de roupagem de mecânica quântica.

TESTE PÓS-PRODUTO			
Aluno (a):	2/2/11/2/2		
Disciplina: FÍSICA	ATIVIDADE EXTRA	Professor: THIAGO CABRAL	Data:
Parte I – Vetores e Decomposição Vetorial 1. Um vetor tem módulo 12 N e forma um ângulo de 45° com o eixo horizontal. Qual é a componente horizontal (Fx) aproximada desse vetor? a) 5 N ☒ b) 8,5 N c) 10,6 N d) 12 N 2. Um vetor de aceleração tem módulo 15 m/s² e inclinação de 30° com o solo. Qual é a componente vertical (Ay)? a) 7,5 m/s² ☒ b) 13 m/s² c) 15 m/s² d) 5 m/s²		Parte III – Física Quântica (Introdução Conceitual) 5. O que é superposição quântica? a) A soma de várias partículas ocupando o mesmo espaço físico ☒ b) Um estado em que a partícula está em mais de uma configuração ao mesmo tempo c) O momento em que a partícula colide com outra d) A variação de massa de uma partícula instável 6. O que acontece quando um sistema quântico em superposição é medido? ☒ a) Ele passa a ter múltiplos estados simultaneamente b) Ele desaparece temporariamente c) Seu estado colapsa em um dos possíveis resultados observáveis d) Ele duplica sua função de onda	
Parte II – Probabilidade 3. Um baralho comum (52 cartas) é embaralhado. Qual a probabilidade de tirar uma carta de ouro? ☒ a) $\frac{1}{4}$ b) $\frac{1}{2}$ c) $\frac{1}{13}$ d) $\frac{3}{4}$ 4. Uma caixa tem 5 bolas numeradas de 1 a 5. Se uma bola é retirada ao acaso, qual é a chance de sair um número ímpar? a) $\frac{1}{5}$ ☒ b) $\frac{3}{5}$ c) $\frac{1}{2}$ d) $\frac{1}{5}$		Parte IV – Criptografia Clássica 7. Em uma cifra de substituição simples, o que é necessário para recuperar a mensagem original? a) Um computador quântico b) A análise do idioma da mensagem ☒ c) A chave usada para a substituição d) Conhecimento em física moderna 8. Por que cifras de substituição simples são consideradas frágeis para proteger informações sigilosas? a) Porque o processo exige acesso a redes de internet seguras ☒ b) Porque podem ser facilmente quebradas com análise de frequência e tentativa e erro c) Porque dependem de máquinas complexas d) Porque não utilizam letras, apenas números	
		Parte V – Criptografia Quântica (Conceitos Iniciais) 9. O protocolo BB84 é um exemplo de: a) Código usado em computadores analógicos b) Técnica de compressão de dados ☒ c) Protocolo de criptografia quântica baseado em fótons polarizados d) Sistema clássico de cifras de substituição	
10. O que torna a criptografia quântica praticamente inviolável? a) Ela não depende de nenhuma chave b) A informação é protegida por campos gravitacionais ☒ c) Qualquer tentativa de interceptação altera o estado da partícula, revelando a espionagem d) Ela usa apenas números primos grandes			

Figuras 14 e 15 – Páginas 1 e 2 do teste pós-produto

É necessário levantar a questão de que o próprio uso do teste preliminar atuou como um revisor do conteúdo, situação essa que não só era esperada como desejada no planejamento da atividade. Ainda assim, é válida a análise de desempenho dos testes. Não só numa análise quantitativa na resolução dos testes, como qualitativa ao longo das atividades.

Os alunos apresentaram no decorrer das aulas um interesse muito grande em rever os conteúdos de Física de anos anteriores, além de apresentarem grande entusiasmo em tentar entender o funcionamento do mundo quântico.

9. Conclusão

Este trabalho propõe uma abordagem inovadora e acessível para o ensino de conceitos de física moderna e segurança da informação no Ensino Médio, por meio da construção e aplicação de um jogo didático baseado no protocolo quântico BB84. A proposta surge em resposta ao desafio contemporâneo de tornar o ensino de física mais atrativo, contextualizado e conectado com os avanços da ciência e da tecnologia.

Ao tratar de temas como superposição quântica, colapso do vetor de estado, medição quântica e preparação de estados, normalmente considerados abstratos e distantes da realidade dos alunos, o jogo atua como uma ponte entre o concreto e o simbólico, entre o lúdico e o conceitual. Ele permite que o aluno experimente situações simuladas de criptografia quântica, enfrentando decisões, observando consequências e compreendendo, na prática, os fundamentos da comunicação segura baseada em fenômenos quânticos.

Ancorado na pedagogia libertadora de Paulo Freire, o trabalho valoriza o aluno como sujeito de conhecimento, promovendo diálogos significativos, construção coletiva do saber e ressignificação de conceitos científicos. A partir da perspectiva histórico-cultural de Vygotsky, foi possível estruturar uma proposta que considera a mediação simbólica como central para a aprendizagem – os qubits representados por macrobits, as escolhas de base de medição, a lógica do jogo – tudo atua como instrumentos culturais que organizam o pensamento dos alunos e permitem a formação de conceitos científicos genuínos.

Além disso, ao utilizar como eixo condutor a metáfora do Gato de Schrödinger, o jogo estimula reflexões sobre a natureza da realidade quântica e o papel do observador, conectando ciência, filosofia e educação. Por meio da simulação da comunicação entre dois participantes, são exploradas noções de interferência, colapso, incerteza e segurança, gerando discussões que transcendem o conteúdo curricular e alcançam temas contemporâneos relevantes para a formação cidadã.

Os resultados obtidos durante a aplicação do jogo se mostraram consistentes com as previsões teóricas do protocolo BB84. A taxa de desacordo entre as bases escolhidas dos alunos permaneceu próxima de 50%, valor esse esperado para um sistema em que as bases de preparação e medição são selecionadas aleatoriamente. Esse resultado evidencia que a dinâmica do jogo foi capaz de reproduzir, de forma satisfatória, o comportamento estatístico fundamental associado à comunicação quântica.

Além disso, se observou uma taxa de recuperação da mensagem original de 100%, uma vez que todos os alunos participantes foram capazes de conseguir reconstruir corretamente a informação transmitida após o processo de comparação das bases compatíveis. Esse resultado reforça a eficácia do jogo como ferramenta didática, demonstrando que a atividade foi capaz não apenas de engajar os estudantes, mas também de promover compreensão operacional do funcionamento do protocolo e de seus mecanismos de segurança.

A avaliação proposta – tanto quantitativa quanto qualitativa – permitiu verificar não apenas a assimilação dos conceitos físicos envolvido, mas também mudanças de atitude dos alunos frente à disciplina, ampliação do interesse pelos temas de física moderna desenvolvimento da capacidade de interpretar modelos simbólicos associados à mecânica quântica.

Entretanto, esses resultados devem ser interpretados com cautela. A pesquisa foi desenvolvida em apenas duas turmas, com um número limitado de participantes, além de uma

pequena variedade sociocultural e financeira, o que restringe a generalização dos achados para outros contextos educacionais. Além disso, fatores como o perfil da turma, a atuação do professor-pesquisador, o tempo disponível para a aplicação da sequência didática e o caráter inovador da atividade podem ter influenciado positivamente o envolvimento dos estudantes.

Outro aspecto a ser considerado é que a avaliação se concentrou nos efeitos imediatos da intervenção, não sendo possível verificar a retenção dos conhecimentos em médio e longo prazo, apenas com este trabalho. Estudos futuros poderão investigar se a aprendizagem observada permanece ao longo do tempo e se a proposta apresenta resultados semelhantes quando aplicada em diferentes escolas, níveis de ensino e contextos socioculturais.

Também é importante reconhecer que o macrobit, embora constitua um recurso eficiente para apresentar os princípios fundamentais do protocolo BB84 em nível didático, não reproduz integralmente os fenômenos físicos envolvidos na manipulação de qubits reais. Trata-se de uma representação pedagógica concebida para reduzir a abstração dos conceitos, preservando seus aspectos conceituais essenciais, mas sem substituir a abordagem formal da Mecânica Quântica.

Por fim, embora os resultados indiquem evidências favoráveis ao uso do Produto Educacional, não se pode atribuir exclusivamente ao jogo didático os avanços observados. A mediação realizada pelo professor, as interações entre os estudantes, o planejamento da sequência didática e os referenciais pedagógicos adotados – especialmente aqueles fundamentados em Ausubel, Vygotsky e Freire – também constituíram elementos relevantes para o processo de aprendizagem. Dessa forma, os resultados devem ser compreendidos como decorrentes da articulação entre esses diferentes fatores, e não apenas na utilização do recurso didático em si.

Como perspectiva futura, pretende-se incorporar à dinâmica do jogo a presença de um terceiro participante no jogo capaz de simular situações de interceptação da comunicação quântica: o espião. A inclusão desse elemento tende a aproximar ainda mais a atividade do comportamento observado em sistemas quânticos reais, uma vez que a tentativa de medição realizada pelo espião provocará alterações e destruições nos macrobits, reproduzindo de maneira mais fiel os efeitos associados ao colapso do estado quântico e à perturbação inevitável causada pela observação.

Este trabalho pretende, assim, contribuir para a ampliação dos horizontes do ensino de física no Ensino Médio, oferecendo uma estratégia viável, de baixo custo, e alinhada às diretrizes da BNCC no que diz respeito à inclusão de conteúdos de ciência contemporânea e ao desenvolvimento de competências científicas, críticas e tecnológicas.

10. Referências Bibliográficas

- ALVES, G. S.; SOARES, A. B. *Geometria Dinâmica: um estudo de seus recursos, potencialidades e limitações através do software Tabulae*. UFF, 2003.
- AUSUBEL, D. P. *Educational Psychology: A Cognitive View*. New York: Holt, Rinehart and Winston, 1968.
- BELISÁRIO, F. B., Inserindo elementos da criptografia quântica no ensino médio, Dissertação de mestrado, orientador, João A M Pereira, UNIRIO, 2019.
- PEREIRA, J. A. M., UM MÓDULO VOLTADO AO ENSINO DO PROTOCOLO BB84 DE CRIPTOGRAFIA QUÂNTICA USANDO, "MACROBITS", Trabalho apresentado no Encontro de Outono da Sociedade Brasileira de Física 2022, USP, São Paulo, 2022
- PEREIRA, J. A. M.; DAMACENO, F. MACROBITS, a teaching tool for quantum cryptography. *Revista do Professor de Física*, Brasília, Brasil, v. 6, n. Especial, p. 529–532, 2022. DOI: 10.26512/rpf.v1i1.46015. Disponível em: <https://periodicos.unb.br/index.php/rpf/article/view/46015>. Acesso em: 20 jul. 2026.
- BRIGAGÃO, G. *Ondas: tudo que você precisa saber para o Enem*. Descomplica, 2016. Disponível em: <https://descomplica.com.br/blog/fisica/resumo-ondas/>
- FREIRE, P. *Pedagogia do Oprimido*. 50 ed. Rio de Janeiro: Paz e Terra, 2021.
- MOREIRA, M. A.; MASINI, E. F. S. *Aprendizagem significativa: a teoria de David Ausubel*. São Paulo: Centauro, 2001.
- PIETROCOLA, M. *A Matemática como estruturante do conhecimento físico*. CBEF, 2002. Disponível em: <https://periodicos.ufsc.br/index.php/fisica/article/download/9297/8588>
- VYGOTSKY, L. S. *A formação social da mente*. São Paulo: Martins Fontes, 2000.
- _____. MINISTÉRIO DA EDUCAÇÃO. SECRETARIA DE EDUCAÇÃO BÁSICA. *Base Nacional Comum Curricular*. Brasília: MEC, 2017. Disponível em: <http://basenacionalcomum.mec.gov.br>
- BENNETT, C. H.; BRASSARD, G. *Quantum cryptography: Public key distribution and coin tossing*. *Theoretical Computer Science*, 560(1):7–11, 2014.
- SCHRÖDINGER, E. *The Present Situation in Quantum Mechanics*. *Proceedings of the American Philosophical Society*, 1935.
- SHANKAR, R. *Principles of Quantum Mechanics*. 2. ed. New York: Springer, 2012
- NIELSEN, M. A.; CHUANG, I. L. *Quantum Computation and Quantum Information*. Cambridge: Cambridge University Press, 2010.
- AUSUBEL, D. P. *Aquisição e retenção de conhecimentos: uma perspectiva cognitiva*. Lisboa: Plátano, 2003.
- BARDIN, L. *Análise de conteúdo*. São Paulo: Edições 70, 2016.
- BOGDAN, R. C.; BIKLEN, S. K. *Investigação qualitativa em educação: uma introdução à teoria e aos métodos*. Porto: Porto Editora, 1994.

MINAYO, M. C. S. *Pesquisa social: teoria, método e criatividade*. 32. ed. Petrópolis: Vozes, 2012.

ZABALA, A. *A prática educativa: como ensinar*. Porto Alegre: Artmed, 1998.

RIGOLIN, Gustavo; RIEZNIK, Andrés Aníbal. Introdução à criptografia quântica. *Revista Brasileira de Ensino de Física*, São Paulo, v. 27, n. 4, p. 517–526, 2005. DOI: 10.1590/S1806-11172005000400004.

SANTOS, Neviton Pereira dos. *A Física do Tunelamento Quântico: uma proposta de organizador prévio para o Ensino Médio*. 2017. Dissertação (Mestrado Nacional Profissional em Ensino de Física) – Universidade Estadual de Feira de Santana, Feira de Santana, 2017. Orientador: José Carlos Oliveira de Jesus.

APÊNDICE: PRODUTO EDUCACIONAL

APRESENTAÇÃO

Este produto educacional é parte integrante da dissertação: ENCRIPAMENTO QUÂNTICO NO ENSINO MÉDIO UTILIZANDO O PROTOCOLO BB84, desenvolvida no âmbito do Programa de Mestrado Nacional Profissional em Ensino de Física, polo 30 – Unirio Sudeste-RJ, como parte dos requisitos necessários à obtenção do título de Mestre em Ensino de Física.

Este material foi elaborado com o objetivo de auxiliar professores da Educação Básica na introdução de conceitos de mecânica quântica e criptografia quântica por meio de uma abordagem lúdica, acessível e de baixo custo. O produto consiste em um jogo didático inspirado no protocolo BB84 de distribuição quântica de chaves, utilizando um dispositivo clássico denominado macrobit para representar analogamente o comportamento de qubits.

A proposta busca aproximar os alunos de temas contemporâneos da ciência, especificamente na área de Física, como computação quântica, segurança digital e transmissão segura de informações, utilizando atividades práticas e interativas capazes de estimular o interesse, a curiosidade, o pensamento crítico e a participação ativa dos estudantes.

O material foi pensado para que possa ser utilizado de forma autônoma por outros professores, sem necessidade de consulta à dissertação original. Desta maneira, o produto educacional apresenta explicações conceituais essenciais, orientações metodológicas, roteiros completos de aplicação, modelos de tabelas e sugestões de avaliação. Caso o professor tenha o desejo de aprofundar o trabalho, é convidado a fazer a leitura completa da dissertação.

A proposta é destinada principalmente a alunos do Ensino Médio, especialmente após conteúdos introdutórios relacionados a vetores, movimento circular uniforme e probabilidade. Sua utilização pode ser destinada também a feiras científicas, clubes de ciência e atividades interdisciplinares envolvendo física e matemática, além de tecnologia e atualidades.

A dinâmica do jogo permite que os alunos experimentem conceitos centrais da mecânica quântica, como superposição de estado, preparação e escolha de bases de medição, colapso do vetor de estado e segurança da criptografia quântica.

O produto promove discussões sobre o impacto social da ciência e da tecnologia na vida contemporânea, especialmente no contexto da segurança digital e da proteção de informações.

É esperado que este material contribua para tornar o ensino de física moderna mais significativo, contextualizado e motivador, aproximando os alunos de temas científicos atuais, normalmente ausente do currículo tradicional, mas que desperta muita curiosidade entre os estudantes.

O presente trabalho foi realizado com o apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – Brasil (CAPES) – código de financiamento 001.

Sumário

1. Introdução	81
2. Fundamentação Teórica.....	82
2.1 Ensino de Física Moderna no Ensino Médio.....	82
2.2 Referencial pedagógico	82
2.3 Conceitos quânticos.....	83
3. O Macrobit.....	84
4. O jogo do encriptamento quântico BB84	85
4.1 Objetivos do jogo	85
4.2 Público-alvo.....	85
4.3 Materiais necessários.....	85
4.4 Organização da turma.....	86
4.5 Etapas do jogo	86
5. Aplicação em Sala de Aula.....	87
5.1 Tempo estimado	87
5.2 Apresentação e regras do jogo.....	87
5.3 Desenvolvimento da dinâmica	87
5.4 Discussões conceituais	88
5.5 Resultados finais.....	88
6. Avaliação da Aprendizagem.....	89
6.1 Avaliação diagnóstica.....	89
6.2 Avaliação durante o jogo.....	89
6.3 Avaliação final.....	89
6.4 Sugestões de questionamentos.....	90
7. Considerações Finais	91
8. Referências	92
9. Apêndices	Erro! Indicador não definido.
APÊNDICE A: Teste pré-produto.....	Erro! Indicador não definido.
APÊNDICE B: Teste pós-produto.....	Erro! Indicador não definido.
APÊNDICE C: Tabela para o Emissor.....	Erro! Indicador não definido.
APÊNDICE D: Tabela para o Receptor	Erro! Indicador não definido.

1. Introdução

O ensino de física moderna no Ensino Médio ainda enfrenta dificuldades relacionadas à abstração dos conceitos e à distância entre os conteúdos abordados e a realidade cotidiana dos estudantes. Temas como mecânica quântica, computação quântica e criptografia quântica normalmente aparecem apenas de maneira superficial nos currículos escolares, apesar de sua crescente importância científica e tecnológica.

Nesse contexto, torna-se fundamental o desenvolvimento de estratégias didáticas capazes de tornar esses conceitos mais significativos e acessíveis. Este produto educacional propõe uma abordagem baseada em atividades investigativas e lúdicas para introduzir conceitos fundamentais da criptografia quântica utilizando analogias clássicas e recursos manipuláveis.

A proposta central deste produto é a utilização de um jogo didático inspirado no protocolo BB84 de distribuição quântica de chaves criptográficas. O jogo utiliza um dispositivo denominado macrobit, criado para simular de maneira acessível alguns comportamentos associados aos qubits.

Ao longo da atividade, os alunos realizam etapas de codificação, compartilhamento de chaves, escolha de bases de medição e descryptografia de mensagens. Durante esse processo, são trabalhados conceitos fundamentais da mecânica quântica e da segurança da informação.

Apesar de ter como pano de fundo a simulação do protocolo BB84 e seja uma abordagem mais direta de conceitos quânticos, o jogo tem como intenção secundária o reforço de conteúdos presentes no currículo-base de Física (como vetores e movimento circular uniforme), e também de Matemática (como probabilidade). Além disso, é esperado obter um maior interesse dos alunos pelas áreas de tecnologia e ciências.

Além do desenvolvimento conceitual, o produto busca promover a participação ativa dos alunos, aprendizagem colaborativa, discussões investigáveis, relações entre ciência, tecnologia e sociedade.

2. Fundamentação Teórica

2.1 Ensino de Física Moderna no Ensino Médio

O ensino de física moderna possui grande relevância na formação científica contemporânea dos alunos. Conceitos relacionados à mecânica quântica, computação quântica e segurança da informação estão cada vez mais presentes na sociedade atual, seja por meio das tecnologias digitais, seja pelo desenvolvimento de novos sistemas computacionais.

Contudo, muitos desses conteúdos não são apresentados de maneira acessível para os alunos da Educação Básica, isso quando são planejados ou, até mesmo, explicados a partir do questionamento de alguns alunos sobre esses temas.

Nesse sentido, o uso de modelos didáticos, analogias e jogos educativos surge como alternativa importante para aproximar os alunos desses assuntos.

2.2 Referencial pedagógico

A proposta deste produto educacional encontra fundamentação principalmente nas contribuições de Lev Vygotsky, David Ausubel e Paulo Freire.

Do ponto de vista freiriano, o aluno é visto como sujeito ativo do processo de aprendizagem. O jogo promove diálogo, participação coletiva e construção compartilhada do conhecimento.

Na perspectiva histórico-cultural de Vygotsky, o macrobit funciona como instrumento mediador da aprendizagem. As representações simbólicas utilizadas no jogo auxiliam os estudantes na construção de conceitos científicos relacionados à mecânica quântica.

Já a aprendizagem significativa de Ausubel contribui para a organização do conteúdo partindo do concreto para o abstrato, permitindo que os alunos estabeleçam relações entre conhecimento prévios e novos conceitos.

2.3 Conceitos quânticos

Durante a aplicação do produto, serão introduzidos alguns conceitos, como:

A. Superposição de estados

Os alunos serão levados a compreender que, em sistemas quânticos, o resultado de uma medida depende da escolha da base utilizada para observação.

B. Colapso do vetor de estado

Ao realizar uma medida, o sistema passa a assumir apenas um dos resultados possíveis.

C. Bases de medição

O jogo utiliza duas bases de medição: base forma e base cor.

Essa escolha permite simular o comportamento probabilístico no protocolo BB84.

3. O Macrobit

O macrobit é um dispositivo didático clássico criado para representar, como um recurso análogo didático, algumas características do comportamento quântico dos qubits.

Fisicamente, o macrobit pode ser construído como cartões com diferentes combinações de forma e cor: quadrado, branco de um lado e preto do outro, e círculo, branco de um lado e preto do outro.

Dependendo da base escolhida pelo receptor, o resultado binário obtido poderá ser diferente.

Embora o macrobit não seja um sistema genuinamente quântico, ele permite representar: a dependência da medida em relação à base escolhida, a ambiguidade de observação, o processo de medição e a simulação conceitual do colapso do vetor de estado. Dessa maneira, o macrobit torna conceitos extremamente abstratos mais acessíveis aos alunos.

É importante destacar também algumas limitações que o macrobit, por ser um dispositivo clássico, possui. O macrobit não apresenta superposição quântica real, então nem sempre uma medida irá gerar ambiguidade (como um círculo branco ou quadrado preto, ambos possuem o mesmo código independente da escolha da base de medição) e, após a medida, não haverá a destruição dos macrobits.

O macrobit portanto se trata de um análogo didático construída para facilitar a compreensão dos conceitos fundamentais envolvidos no protocolo BB84.

4. O jogo do encriptamento quântico BB84

4.1 Objetivos do jogo

Os objetivos principais do jogo são:

- Introduzir conceitos básicos de mecânica quântica
- Trabalhar segurança da informação
- Simular o protocolo BB84
- Desenvolver aprendizagem colaborativa
- Estimular o interesse pela física moderna e, como extensão, a física clássica da base curricular do Ensino Médio

4.2 Público-alvo

Estudantes do Ensino Médio que já tenham tido contato com assuntos como: vetores, movimento circular uniforme e probabilidade. Como a divisão do currículo-base do Ensino Médio não é igualmente distribuída pelas séries em todos os colégios, o público-alvo estará em séries diferentes a depender do colégio.

4.3 Materiais necessários

- Macrobits
- Folhas do emissor
- Folhas do receptor
- Pasta ou sacola para os macrobits
- Quadro branco ou projetor

4.4 Organização da turma

A turma deve ser organizada em duplas. Cada dupla será composta por um emissor e um receptor.

4.5 Etapas do jogo

Etapa 1: Escolha da mensagem

- O emissor escolhe uma sequência de três letras utilizando o alfabeto genômico: A, T, C e G.
- Cada símbolo é convertido em bits utilizando a tabela de codificação presente na folha do emissor.

Etapa 3: Preparação dos macrobit

- O emissor irá sortear (ou escolher de forma aleatória) um conjunto de 20 macrobits

Etapa 3: Escolha das bases

- Para cada macrobit, o emissor escolhe aleatoriamente uma base: forma ou cor.
- Cada um dos macrobits irá gerar um bit correspondente a base de medição escolhida

Etapa 4: Medição do receptor

- O receptor escolhe aleatoriamente uma base de medição para cada macrobit recebido.

Etapa 5: Comparação pública das bases

- Emissor e receptor compartilham apenas as bases utilizadas
- Quando a base escolhida pelo receptor coincide com a utilizada pelo emissor, o bit é obtido corretamente.
- Quando as bases são incompatíveis, o bit deve ser descartado.

Etapa 6: Descriptografia da mensagem

- Receptor utiliza os bits compatíveis para reconstruir a mensagem original

5. Aplicação em Sala de Aula

5.1 Tempo estimado

A aplicação completa pode ser realizada em, aproximadamente, 50 min.

- 15 min: apresentação e regras do jogo
- 20 min: dinâmica do jogo
- 15 min: aquisição dos resultados e considerações finais

5.2 Apresentação e regras do jogo

O professor pode iniciar a atividade levantando a discussão sobre:

- segurança digital
- senhas
- aplicativos de mensagem
- criptografia

Sugestões de perguntas:

- Como as mensagens do WhatsApp são protegidas?
- É possível transmitir informações de forma totalmente segura?

5.3 Desenvolvimento da dinâmica

- Organizar os estudantes em duplas
- Distribuir os materiais
- Explicar rapidamente as regras
- Permitir que os alunos realizem a dinâmica

- Mediar dúvida apenas quando necessário, permitindo que os estudantes interajam entre si favorecendo a aprendizagem colaborativa

5.4 Discussões conceituais

Após a dinâmica, o professor pode utilizar a experiência com o jogo para explicar os conceitos:

- Superposição
- Colapso do vetor de estado
- Bases de medição
- Segurança quântica

5.5 Resultados finais

O professor pode, juntamente com as duplas, determinar:

- A taxa de compatibilidade entre as bases de medição (esperando um valor próximo a 50%)
- O percentual de duplas que conseguiu determinar a mensagem original do emissor

Ao término, o professor pode trazer para as considerações finais os motivos das escolhas por um alfabeto reduzido (de 4 letras: A, C, G e T) e uma mensagem reduzida (de três letras), qual seria a viabilidade de se fazer uma dinâmica com um alfabeto mais extenso e a qual seria a quantidade de bits que seriam necessários para esse alfabeto mais extenso.

6. Avaliação da Aprendizagem

6.1 Avaliação diagnóstica

Antes da atividade, é recomendado a aplicação de um questionário investigativo, desejando determinar a base conceitual dos alunos em:

- Probabilidade
- Vetores
- Movimento circular uniforme
- Criptografia

6.2 Avaliação durante o jogo

Durante o jogo, o professor pode fazer uma avaliação qualitativa, observando:

- Participação dos alunos
- Interação entre as duplas
- Capacidade de interpretação das tabelas
- Argumentação dos estudantes

6.3 Avaliação final

Após a aplicação do jogo, é sugerido ao professor:

- Aplicação de pós-teste
- Discussão coletiva
- Reflexões sobre segurança digital

Como extensão, o professor pode, através da obtenção dos resultados do pós-teste identificar as dificuldades residuais dos conteúdos desejados e planejar um reforço dos conceitos numa aula posterior.

6.4 Sugestões de questionamentos

- O que acontece quando o emissor e o receptor utilizam bases diferentes?
- Por que o protocolo BB84 é considerado seguro?
- Qual a relação entre medida e colapso do vetor de estado?
- O que aconteceria caso uma terceira pessoa tentasse interceptar a mensagem?

7. Considerações Finais

Este produto educacional apresenta uma proposta didática acessível e simbólica de baixo custo para o ensino de conceitos introdutórios da mecânica quântica e criptografia quântica no Ensino Médio, além de reforçar assuntos presentes no currículo-base de Física.

Todas as tabelas, testes e instrumentos de avaliação propostos encontram-se disponibilizados nos Apêndice deste material. Contudo, esses recursos devem ser compreendidos como sugestões de orientação, cabendo ao professor adaptá-los, modifica-los ou ampliá-los de acordo com seus objetivos pedagógicos, levando em consideração as características da turma e os interesses específicos do contexto educacional em que serão aplicados.

Por abordar conteúdos tradicionalmente presentes no currículo do Ensino Médio, este produto educacional possibilita ao professor atribuir maior significado e aplicabilidade a conceitos frequentemente trabalhados sem inovação na contextualização ou, até mesmo, sem contextualização moderna. Sua implementação pode ocorrer tanto após a abordagem formal desses conteúdos, atuando como instrumento de consolidação da aprendizagem, quanto como um projeto investigativo e lúdico, incentivando os estudantes a identificar, analisar e relatar situações do cotidiano nas quais os conhecimentos estudados se fazem presentes. Desta forma, busca-se promover uma aprendizagem mais contextualizada, significativa e alinhada às demandas da educação contemporânea.

A proposta apresentada não pretende constituir um modelo rígido de aplicação, mas sim uma ferramenta flexível capaz de inspirar novas práticas pedagógicas. A partir das adaptações realizadas pelos próprios professores, o produto pode assumir diferentes formatos e objetivos, ampliando seu potencial de utilização e contribuindo para a diversificação das estratégias de ensino de Física no Ensino Médio.

Assim sendo, este produto educacional busca não apenas auxiliar o ensino dos conteúdos abordados, mas também incentivar a adoção de práticas pedagógicas mais contextualizadas, investigativas, lúdicas e significativas, fortalecendo o protagonismo dos alunos na construção do conhecimento científico.

8. Referências

AUSUBEL, David. Aquisição e retenção de conhecimentos: uma perspectiva cognitiva. Lisboa: Plátano, 2003.

BENNETT, Charles H.; BRASSARD, Gilles. Quantum cryptography: Public key distribution and coin tossing. Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, 1984.

DIRAC, Paul A. M. Os princípios da mecânica quântica. Lisboa: Fundação Calouste Gulbenkian.

FREIRE, Paulo. Pedagogia da autonomia. São Paulo: Paz e Terra.

NIELSEN, Michael A.; CHUANG, Isaac L. Computação quântica e informação quântica.

VYGOTSKY, Lev. A formação social da mente. São Paulo: Martins Fontes.

APÊNDICE A: Teste pré-produto

TESTE PRELIMINAR

Aluno (a): _____

Disciplina:
FÍSICA

**ATIVIDADE
EXTRA**

Professor:
THIAGO CABRAL

Data:

Parte I – Vetores e Decomposição Vetorial

1. Um vetor de força $\vec{F}$ tem intensidade de 10 N e forma um ângulo de 30° com o eixo horizontal. Qual é o valor aproximado da projeção horizontal (F_x) desse vetor?

- a) 5 N
- b) 8,7 N
- c) 10 N
- d) 7,5 N

2. A base alfa é composta por dois vetores unitários, A e B , perpendiculares entre si. O vetor A aponta para o leste, enquanto o vetor B aponta para o norte. Considerando o vetor $R = A + B$, assinale a alternativa correta:

- a) A intensidade de R vale 1 e sua direção forma um ângulo de 45° com a direção leste.
- b) A intensidade de R vale 2 e sua direção forma um ângulo de 90° com a direção norte.
- c) A intensidade de R vale $\sqrt{2}$ e sua direção forma um ângulo de 45° com a direção leste.
- d) A intensidade de R vale $\sqrt{2}$ e sua direção forma um ângulo de 0° com a direção leste.

3. Seja agora uma nova base β composta pelos vetores unitários $\vec{A}'$ e $\vec{B}'$, obtidos ao girar a base original α (formada por $\vec{A}$ e $\vec{B}$) de 45° no sentido anti-horário em relação ao plano horizontal.

Admita o vetor $\vec{R}$, que possui projeções (1,1) na base original α , da questão anterior.

Com base nessas informações, assinale a alternativa correta sobre as projeções do vetor $\vec{R}$ na base β :

- a) As projeções de $\vec{R}$ permanecem iguais: (1,1), pois a rotação da base não altera as projeções.
- b) As projeções de $\vec{R}$ na nova base são (1,0), indicando que ele aponta apenas na direção de $\vec{A}'$.
- c) As projeções de $\vec{R}$ na nova base são $(0, \sqrt{2})$, indicando que ele aponta apenas na direção de $\vec{B}'$.
- d) As projeções de $\vec{R}$ na nova base são $(\sqrt{2}/2, \sqrt{2}/2)$, pois o vetor continua com módulo 1 e é igualmente projetado nas direções $\vec{A}'$ e $\vec{B}'$.

Parte II – Probabilidade

4. Um dado comum (seis faces numeradas de 1 a 6) é lançado. Qual é a probabilidade de sair um número par?

- a) $\frac{1}{6}$
- b) $\frac{1}{2}$
- c) $\frac{2}{3}$
- d) $\frac{5}{6}$

5. Em um jogo de cartas, Thiago explica que, ao retirar uma carta de um baralho especial com apenas cartas vermelhas, a probabilidade de sair uma carta vermelha é igual a 1.

Com base nessa informação, é correto afirmar que:

- a) Uma carta vermelha pode nunca ser sorteada.
- b) A ocorrência de sair uma carta vermelha é certa.
- c) Nada garante que uma carta vermelha será sorteada.
- d) As chances de sair uma carta vermelha são de 50%.

Parte II – Movimento Circular Uniforme

6. Um ciclista percorre uma pista circular de raio constante com velocidade escalar constante. Sobre esse movimento, é correto afirmar que:

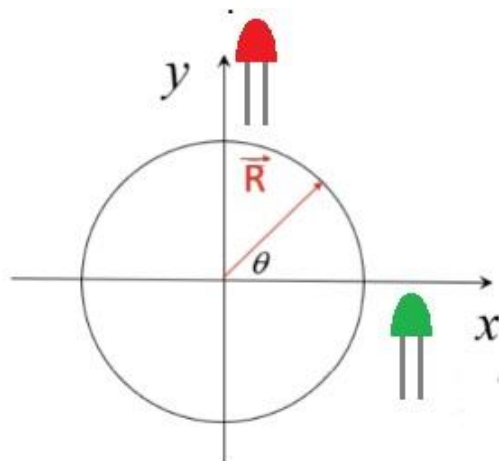
- a) A velocidade vetorial do ciclista não muda, pois sua velocidade escalar é constante.
- b) A aceleração do ciclista é nula, já que ele está em velocidade constante.
- c) O movimento do ciclista é retilíneo uniforme, pois ele não muda de direção.
- d) A velocidade escalar do ciclista é constante, mas sua velocidade vetorial muda o tempo todo.

7. Um ponto em movimento circular uniforme completa 5 voltas em 10 segundos. Com base nesses dados, qual é o valor da frequência e do período desse movimento?

- a) Frequência = 0,5 Hz; Período = 2 s
- b) Frequência = 2 Hz; Período = 0,5 s
- c) Frequência = 5 Hz; Período = 10 s
- d) Frequência = 10 Hz; Período = 5 s

ENUNCIADO PARA AS QUESTÕES 8 e 9

A figura abaixo apresenta um gráfico com uma circunferência de raio 1 e centro na origem (0,0).



Esse gráfico representa a cor resultante emitida por um LED devido a combinação dos brilhos de duas componentes: vermelho (eixo y) e verde (eixo x). A partir disso, podem ser feitas as afirmações:

- Nos pontos (0,1) e (0,-1) o LED apresentará a cor vermelha com brilho máximo (e brilho verde nulo).
- Nos pontos (1,0) e (-1,0) o LED apresentará a cor verde com brilho máximo (e brilho vermelho nulo).
- Em todos os pontos da circunferência, o LED irá emitir uma combinação entre a luz verde e a luz vermelha. Quando a intensidade de ambas as cores for a mesma, a LED assume a cor amarela.

8. Qual das coordenadas a seguir apresentará o LED quando assume a cor amarela?

- a) $(\frac{\sqrt{2}}{2}, \frac{\sqrt{2}}{2})$
- b) $(\sqrt{2}, \sqrt{2})$
- c) (0,1)
- d) (1,1)

9. O LED é fotografado em momentos aleatórios fornecendo x imagens, onde x é um número muito grande.

Nessa situação podemos concluir que o que aparecerá mais vezes nas fotografias é o:

- a) LED vermelho.
- b) LED amarelo.
- c) LED verde.
- d) LED apagado.

10. Admita que o eixo xy da base α seja rotacionado em 45° no sentido anti-horário para dar origem a uma nova base β , de eixos $x'y'$.

Nesta nova base β , a cor amarela corresponde a quais coordenadas?

- a) (0,1)
- b) (1,0)
- c) $(\sqrt{2}, 0)$
- d) $(0, \sqrt{2})$

11. Um método comum para determinar se um tipo de tecido é ou não original, é o uso de um tipo especial de tinta reagente. Essa tinta é invisível quando aplicada, mas quando em contato com o tecido ela assume uma coloração amarela por alguns instantes, depois assume uma coloração verde ou vermelha, dependendo do tipo de material. Após isso, uma reação química ocorre, tornando a tinta apenas água e incolor, não manchando assim o tecido.

Esse teste só pode ser feito uma única vez, já que a primeira reação química altera permanentemente a natureza molecular do tecido.

Qual das afirmações a seguir está de acordo com a característica desse tipo de teste?

- a) É possível aplicar o teste novamente para revelar uma nova cor.
- b) A cor só é conhecida no momento da aplicação, após essa reação, o estado do tecido se altera de forma irreversível.
- c) Após o teste é possível retornar o tecido para o estado inicial pré-teste.
- d) Era possível saber o resultado do teste antes mesmo de aplicar a tinta.

DISCURSIVA

12. Imagina que você e seu melhor amigo têm um código secreto pra conversar sem que ninguém mais entenda. Isso é mais ou menos o que a criptografia faz na internet!

Agora, pense e responda:

Por que você acha que a criptografia é importante quando a gente usa redes sociais, faz compras online ou envia mensagens? Você conhece alguma brincadeira ou jogo que envolva a criptografia?

GABARITO

- 1. B**
- 2. C**
- 3. B**
- 4. B**
- 5. B**
- 6. D**
- 7. A**
- 8. A**
- 9. B**
- 10. B**
- 11. B**
- 12. Mini-redação**

APÊNDICE B: Teste pós-produto

TESTE PÓS-PRODUTO

Aluno (a): _____

Disciplina:
FÍSICA

**ATIVIDADE
EXTRA**

Professor:
THIAGO CABRAL

Data:

Parte I – Vetores e Decomposição Vetorial

1. Um vetor tem módulo 12 N e forma um ângulo de 45° com o eixo horizontal. Qual é a componente horizontal (F_x) aproximada desse vetor?

- a) 6 N
- b) 8,5 N
- c) 10,6 N
- d) 12 N

2. Um vetor de aceleração tem módulo 15 m/s^2 e inclinação de 30° com o solo. Qual é a componente vertical (A_y)?

- a) $7,5 \text{ m/s}^2$
- b) 13 m/s^2
- c) 15 m/s^2
- d) 5 m/s^2

Parte II – Probabilidade

3. Um baralho comum (52 cartas) é embaralhado. Qual a probabilidade de tirar uma carta de ouros?

- a) $\frac{1}{4}$
- b) $\frac{1}{2}$
- c) $\frac{1}{13}$
- d) $\frac{3}{4}$

4. Uma caixa tem 5 bolas numeradas de 1 a 5. Se uma bola é retirada ao acaso, qual é a chance de sair um número ímpar?

- a) $\frac{2}{5}$
- b) $\frac{3}{5}$
- c) $\frac{1}{2}$
- d) $\frac{1}{5}$

Parte III – Física Quântica (Introdução Conceitual)

5. O que é superposição quântica?

- a) A soma de várias partículas ocupando o mesmo espaço físico
- b) Um estado em que a partícula está em mais de uma configuração ao mesmo tempo
- c) O momento em que a partícula colide com outra
- d) A variação de massa de uma partícula instável

6. O que acontece quando um sistema quântico em superposição é medido?

- a) Ele passa a ter múltiplos estados simultaneamente
- b) Ele desaparece temporariamente
- c) Seu estado colapsa em um dos possíveis resultados observáveis
- d) Ele duplica sua função de onda

Parte IV – Criptografia Clássica

7. Em uma cifra de substituição simples, o que é necessário para recuperar a mensagem original?

- a) Um computador quântico
- b) A análise do idioma da mensagem
- c) A chave usada para a substituição
- d) Conhecimento em física moderna

8. Por que cifras de substituição simples são consideradas frágeis para proteger informações sigilosas?

- a) Porque o processo exige acesso a redes de internet seguras
- b) Porque podem ser facilmente quebradas com análise de frequência e tentativa e erro
- c) Porque dependem de máquinas complexas
- d) Porque não utilizam letras, apenas números

Parte V – Criptografia Quântica (Conceitos Iniciais)

9. O protocolo BB84 é um exemplo de:

- a) Código usado em computadores analógicos
- b) Técnica de compressão de dados
- c) Protocolo de criptografia quântica baseado em fótons polarizados
- d) Sistema clássico de cifras de substituição

10. O que torna a criptografia quântica praticamente inviolável?

- a) Ela não depende de nenhuma chave
- b) A informação é protegida por campos gravitacionais
- c) Qualquer tentativa de interceptação altera o estado da partícula, revelando a espionagem
- d) Ela usa apenas números primos grandes

GABARITO

- 1. B**
- 2. A**
- 3. A**
- 4. B**
- 5. B**
- 6. C**
- 7. C**
- 8. B**
- 9. C**
- 10. C**

APÊNDICE C: Tabela para o Emissor

Tabela para o Emissor (BB84)

Tabela A

Código de dois bits:	Operação XOR:	Leituras de M-bits:	
A = 0 0	$0 + 0 = 0$	Cor	Branco = "0"
T = 0 1	$0 + 1 = 1$		Preto = "1"
C = 1 0	$1 + 0 = 1$	Forma	Círculo = "0"
G = 1 1	$1 + 1 = 0$		Quadrado = "1"

1) Mensagem (escolha qualquer combinação de três caracteres entre A T C G):

--	--	--

2) Codifique a mensagem em uma sequência binária de seis caracteres usando a primeira coluna da tabela A:

--	--	--	--	--	--

3) Monte um conjunto de 25 M-bits e fixe-os no suporte.

4) Construa uma chave com seu parceiro para criptografar a mensagem codificada em 2.

- Selecione e anote na 2ª coluna da tabela B, 15 bases para ler a sequência de M-bits.
- Escreva a representação binária correspondente na 3ª coluna da tabela B, após a 3ª coluna da tabela A.
- Aguarde os anúncios do receptor para preencher a 4ª coluna da tabela B da outra página marcando S sempre que ele escolher a mesma base que você.

5) Chave – pegue os seis primeiros resultados da 3ª coluna da tabela B se a 4ª coluna estiver marcada por S:

--	--	--	--	--	--

6) Use as sequências binárias que representam a mensagem codificada em (2) e a chave de criptografia em (5) como entradas para a operação XOR seguindo a segunda coluna da tabela A e escreva os resultados na linha designada para a mensagem criptografada.

Mensagem codificada (2)						
Chave de criptografia (5)						

Mensagem criptografada						
------------------------	--	--	--	--	--	--

7) Anuncie os bits da mensagem criptografada ao Receptor

APÊNDICE D: Tabela para o Receptor

Tabela para o Receptor (BB84)

Tabela A

Código de dois bits:	Operação XOR:	Leituras de M-bits:	
A = 0 0	0 + 0 = 0	Cor	Branco = "0"
T = 0 1	0 + 1 = 1		Preto = "1"
C = 1 0	1 + 0 = 1	Forma	Círculo = "0"
G = 1 1	1 + 1 = 0		Quadrado = "1"

1) Construa uma chave com seu parceiro.

- Selecione e anote na 2ª coluna da tabela B, 15 bases para ler a sequência de M-bits.
- Leia os M-bits anexados ao suporte conforme preparado pelo Emissor, tomando nota de sua representação binária correspondente na 3ª coluna da tabela B, após a 3ª coluna da tabela A.

2) Anuncie a base que você usou para ler os M-bits para o Emissor marcando S na 4ª coluna da tabela B sempre que houver acordo.

3) Chave – pegue os seis primeiros resultados da 3ª coluna da tabela B se a 4ª coluna estiver marcada por S:

--	--	--	--	--	--

4) Peça ao Emissor a sequência que representa a mensagem criptografada:

--	--	--	--	--	--

5) Use as sequências binárias que representam a chave de criptografia em (3) e a mensagem criptografada em (4) como entradas para a operação XOR seguindo a segunda coluna da tabela A e escreva os resultados na linha designada para a mensagem descriptografada.

Chave de criptografia (3)						
Mensagem criptografada (2)						

Mensagem descriptografada						
---------------------------	--	--	--	--	--	--

6) Decodifique a mensagem decifrada usando a 1ª coluna da tabela A:

--	--	--

7) Anuncie a mensagem em (6) para o Emissor.