Simulação da Criptografia Quântica

Autores: Ana Terra Vieira Costa[1], Rafaelle da Silva Souza (Orientadora)

Instituto Federal da Bahia campus Salvador - Rua Emídio dos Santos, S/N - Salvador, BA

1 INTRODUÇÃO

O processo de cifrar mensagens ocorre há milênios. Registros datam de aproximadamente 1900 a.C., quando um escriba egípcio alterou símbolos para ocultar informações (IBM, 2024; SILVA, 2019). Ao longo dos séculos, as técnicas evoluíram até sistemas como a Máquina Enigma e a criptografia computacional.

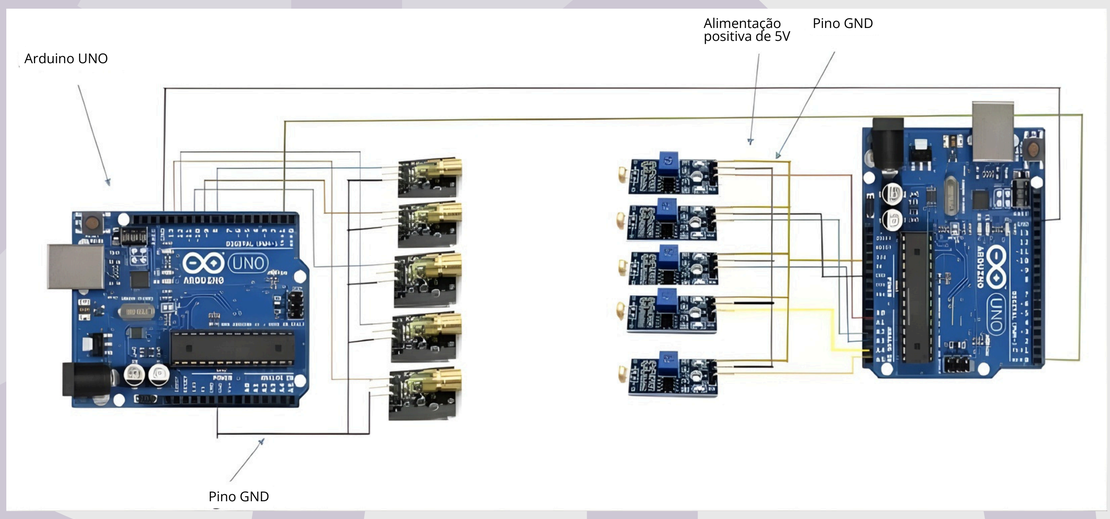
A criptografia quântica representa um avanço teórico e prático ao oferecer segurança baseada em princípios físicos, diferentemente da segurança algorítmica da criptografia clássica (RIGOLIN; RIEZNIK, 2005). Protocolos como BB84 e E91 demonstram a viabilidade da distribuição de chaves com detecção de interceptação (BENNETT; BRASSARD; MERMIN, 1992).

Contudo, a implementação experimental desses protocolos requer equipamentos e detectores de alto custo, o que limita sua utilização. Diante disso, o presente projeto propõe implementar e avaliar um protótipo baseado em Arduino que transmita sequências binárias por pulsos de laser, servindo como recurso didático de baixo custo para QKD (Distribuição de Chaves Quânticas).

2 MATERIAIS E METÓDOS

Para ilustrar a criptografia quântica com Arduino baseada em fótons, foram utilizados: duas placas Arduino Uno, display LCD, protoboard, cinco módulos laser, cinco módulos receptores (LDR) e jumpers. O sistema é composto por dois Arduinos (transmissor e receptor). No transmissor, cinco diodos laser operam para emitir sinais luminosos. No receptor, cinco LDRs organizados em matriz detectam a intensidade da luz recebida.

Imagem 1 – Esquema do sistema de criptografia quântica com Arduino, utilizando cinco diodos laser no transmissor e uma matriz de fotorresistores (LDRs) no receptor para a emissão e detecção de fótons.



Fonte: Autoria Própria

Durante a IV Semana Quântica, um total de 340 estudantes do ensino médio participaram de um questionário estruturado para avaliar a percepção dos alunos sobre segurança digital e criptografia quântica

3 DESENVOLVIMENTO

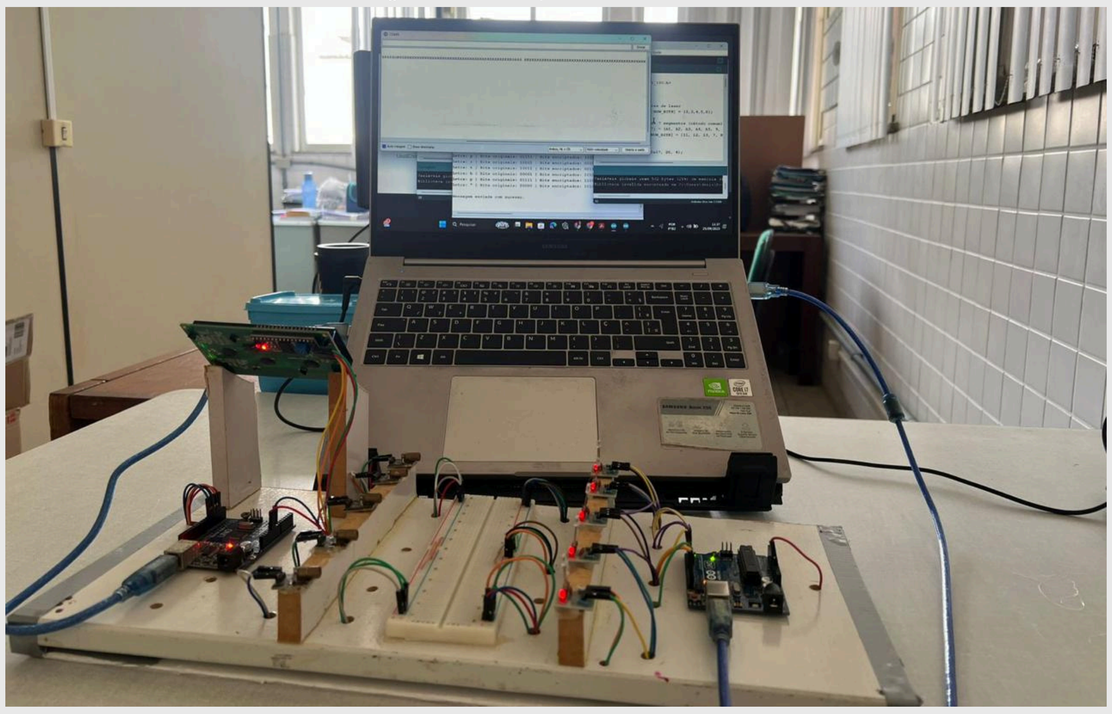
O desenvolvimento ocorreu em duas etapas: modelagem conceitual e implementação com validação experimental. Na etapa conceitual, foram estudados protocolos de QKD, especialmente o BB84, para compreender transmissão de qubits e detecção de interceptação. A partir disso, definiu-se uma adaptação didática baseada em pulsos luminosos. Na implementação, foi montado um sistema com dois Arduino Uno, em quê o transmissor gera sequências binárias e aciona cinco diodos laser e o receptor é matriz de cinco LDRs que converte luz em sinais elétricos interpretados pelo microcontrolador.

Foi desenvolvido um código em linguagem C/C++ para:

- Gerar sequências binárias;
- Converter os bits em sinais de acionamento dos lasers;
- Ler os valores analógicos recebidos pelos LDRs;
- Reconstruir a mensagem original.

Além disso, durante a IV Semana Quântica, o criptografia quântica foi apresentado a estudantes do ensino médio, permitindo observar sua aplicabilidade como ferramenta didática e coletar dados sobre percepção e compreensão do tema.

Imagem 2 – Protótipo em funcionamento



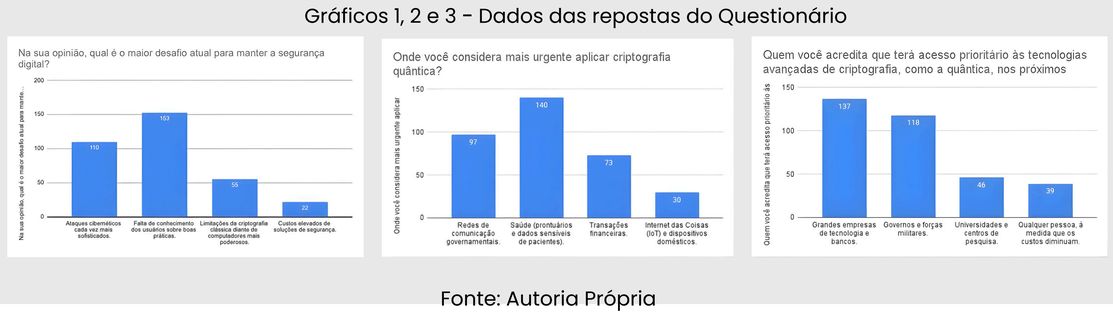
Fonte: Autoria Própria

4 RESULTADOS

O sistema demonstrou viabilidade didática na simulação de princípios da QKD. Foi capaz de transmitir mensagens binárias com **taxa média de 9,6 kbps e tempo médio de resposta de 47 ms.**

O questionário indicou interesse dos estudantes e reconhecimento das limitações da criptografia clássica. Os resultados confirmam a hipótese do projeto: há curiosidade científica no ensino médio, mas lacunas conceituais sobre criptografia quântica.

Gráficos 1, 2 e 3 - Dados das repostas do Questionário



Fonte: Autoria Própria

5 CONCLUSÃO

O projeto demonstrou que é possível explorar conceitos de criptografia quântica de forma acessível, utilizando Arduino como recurso de baixo custo. O sistema mostrou-se capaz de transmitir informações em forma binária, aproximando estudantes da Física Moderna e das aplicações tecnológicas contemporâneas.

REFERÊNCIAS

1.BENNETT, C. H.; BRASSARD, G. Quantum cryptography: Public key distribution and coin tossing. In: Proceedings of IEEE International Conference on Computers, Systems and Signal Processing. Bangalore, India, 1984. p. 175–179. 2. The history of cryptography. IBM, 2024. 3.RIGOLIN, G; RIEZNIK, A. A. Introdução à criptografia quântica. Revista Brasileira de Ensino de Física, v. 27, n. 4, p. 517–526, 2005. 4.SILVA, Willian Wallace de Matteus. A evolução da criptografia e suas técnicas ao longo da história. Instituto Federal Goiano, 2019.

Quantum cryptography Icon; Fonte: Canva