Simpósio de Integração Acadêmica
Inteligência Artificial: A Nova Fronteira da Ciência Brasileira
SIA UFV Virtual 2020

CÓDIGOS QUÂNTICOS E CRIPTOGRAFIA PÓS-QUÂNTICA

Universidade Federal de Viçosa

PEREIRA, G. F , (DMA/UFV)-guilherme.flaviano@ufv.br; Orientador: MOURA, A. O, (DMA/UFV)-allan.moura@ufv.br

Palavra-chave: Criptografia

Matemática Aplicada – Ciências Exatas e Tecnológicas

Pesquisa

Introdução

Na tentativa de buscar sistemas de criptografia mais eficientes para que o envio e recebimento de informações se tornasse mais seguro, surgiu a Criptografia Pós-Quântica. Este tipo de criptografia se torna mais eficaz, devido a possibilidade de se construírem computadores quânticos que são capazes de atacar sistemas complexos de segurança. Nosso estudo consistiu em um profundo estudo desta criptografia.

Objetivos

Aprofundar os conhecimentos sobre a Teoria dos códigos, Criptografia Clássica e Criptografia Pós-Quântica, especificamente estudando princípios inicias sobre os códigos corretores de erros

Material e Métodos

Utilizamos como objeto de pesquisa livros e artigos com conteúdos voltados para as áreas que a criptografia pós-quântica abrange, como por exemplo a Teoria dos códigos, a mecânica quântica, códigos corretores de erros, entre outros.

Resultados e Discussão

Para se chegar a um conhecimento mais preciso em criptografia pós-quântica, foi necessário entendermos alguns conceitos e teorias muito importantes para a construção desta teoria. Nossa primeira abordagem foi sobre a Teoria dos Códigos, com ênfase nos códigos lineares. Eles podem ser definidos como a seguir.

Definição: Um código $C \subset K^n$ será chamado de código linear se for um subespaço vetorial de K^n, onde K é um corpo finito com q elementos tomado como alfabeto e n é dimensão de K.

Os códigos quânticos corretores de erros estão baseados nestes códigos. Os códigos quânticos são utilizados teoricamente em problemas na construção dos computadores quânticos.

Uma outra abordagem foi sobre os códigos quânticos, especialmente o código de Shor. Este código reduz significativamente o tempo de fatoração de números inteiros muito grande, o que computadores faz em tempos muito elevados.

Por fim, aprofundamos no estudo dos sistemas de criptografia baseados em código corretores de erros. O principal deles é sistema de criptografia McEliece, que consiste na utilização de duas chaves, uma pública e uma privada, esta última somente o proprietário das chaves tem o conhecimento dela. Esta chave é utilizada para decifrar os textos cifrados, que são texto onde se introduziram erros.

Deste sistema de criptografia, originou-se outros como o de Neiderreiter, esquema de assinatura CFS, entre outros.

Conclusões

A partir deste estudo, vemos que existem alternativas que são mais seguras para manter nossas informações em segurança, embora esses sistemas ainda estejam em desenvolvimento. Eles apresentam um grande avanço nos estudos sobre a criptografia e a segurança no envio e recebimento de mensagens, e futuramente podem ser a criptografia mais utilizada.

Bibliografia

1 - Bernstein, D. J; Buchmann, J; Dahmen, D. Post-Quantum Cryptography Springer-Verlag Berlin Heidelberg, 2009

2 – Hefez, A; Villela, M.L.T., Códigos Corretores de Erros, Rio de Janeiro, IMPA, 2002

3 - Lavor, C. C; Alves, M. M. S; Siqueira, R. M; Costa, S. I. R., Uma Introdução à Teoria de Códigos, Sociedade Brasileira de Matemática Aplicada e Computacional, São Carlos, 2006.

Apoio Financeiro

Conselho Nacional de Desenvolvimento Científico e Tecnológico - CNPq

Agradecimentos

Agradeço primeiramente a Deus por eu ter participado desta pesquisa, ao Prof. Allan de Oliveira Moura pela oportunidade dada e ao CNPq, por ter patrocinado nossa pesquisa.