Criptografia Pós-Quântica com Códigos Corretores de Erros

UNIVERSIDADE DE SÃO PAULO
Instituto de Matemática e Estatística
Departamento de Ciência da Computação

Autor: Rafael Misoczki
Orientador: Prof. Dr. Paulo S. L. M. Barreto (Poli-USP)

Introdução e Objetivo

A maioria das soluções criptográficas utilizadas atualmente é embasada em problemas relacionados à teoria dos números, tal como o de fatoração de números inteiros em primos, no caso do Algoritmo RSA, e o de logaritmos discretos, para criptografia baseada em curvas elípticas. Porém, sabe-se que esse tipo de solução é vulnerável a ataques provenientes de computadores quânticos [Shor 1994]. Nesse contexto, é sugerida a utilização do Sistema Criptográfico McEliece [McEliece 1978] que, ao apoiar-se em problemas pertinentes à teoria da codificação (mais especificamente de decodificação de mensagens com erros aleatórios), tem se mostrado seguro inclusive neste cenário (não é conhecido algoritmo, seja quântico ou clássico, que resolve tal problema em tempo polinomial), recebendo então, a classificação de *pós-quântico*.

Baseado nesses fatos, o objetivo deste trabalho é analisar o Sistema Criptográfico McEliece, desenvolver uma *Biblioteca Criptográfica Pós-Quântica* que opere segundo esses preceitos, além de propor maneiras eficientes de se implementar representações e simular as operações de estruturas algébricas, tais como Corpos Finitos, necessárias ao sistema.

Biblioteca Criptográfica Pós-Quântica

Por ser baseada no Sistema Criptográfico McEliece, a Biblioteca desenvolvida como aplicação desse estudo herdou algumas características particulares desse sistema. Como principais, podemos citar a segurança perante ataques de Computadores Quânticos (ilustrada por meio da Figura 1), grande eficiência computacional e o tamanho considerável de suas chaves. A Implementação foi realizada em linguagem de programação Java, visando a questão da portabilidade do sistema.

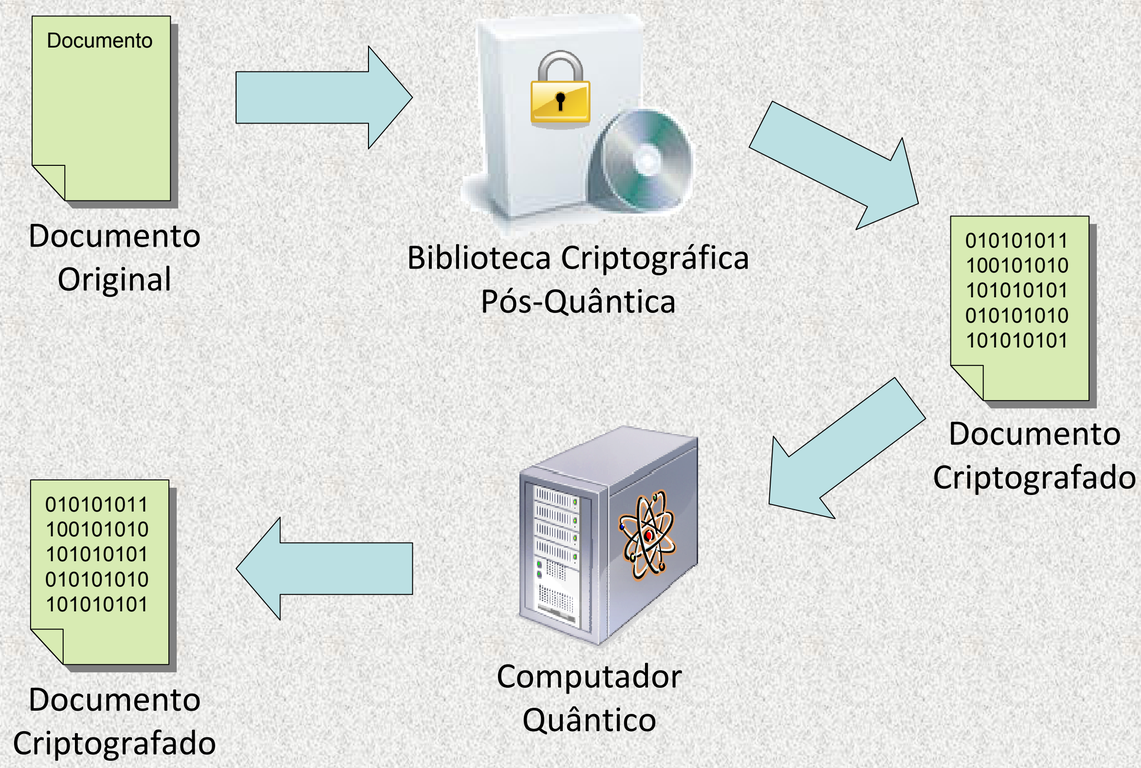

Figura 1: Ineficiência de Ataques Quânticos

A seguir, temos uma comparação entre os sistemas RSA, Curvas Elípticas e McEliece, para um mesmo nível de segurança:

	RSA	Curvas Elípticas	McEliece
É seguro perante ataques de computadores quânticos?	Não	Não	Sim
Eficiência Algorítmica	$O(n^3)$	$O(n^3)$	$O(n^2)$
Tamanho das Chaves	1024 bits	160 bits	88 KB

Tabela 1: Comparação entre McEliece e RSA/Curvas Elípticas

Resultados obtidos

Ao analisar e implementar o Sistema Criptográfico McEliece, foi possível verificar algumas de suas particularidades, tais como eficiência algorítmica e a grande extensão de suas chaves, além de prover uma compilação relevante para pesquisas relacionadas a este sistema. Com relação à implementação das estruturas e operações algébricas, foi possível empregar soluções bastante eficientes. Por exemplo, para as operações de soma de elementos de corpos finitos, utilizamos uma abordagem que resume tal cálculo à operação de ou-exclusivo (XOR), e para a multiplicação, a consultas a tabelas pré-calculadas. Outras operações, tais como módulo polinomial, teste de irredutibilidade e determinação do inverso multiplicativo, também foram implementadas de maneira otimizada, resultando em um sistema criptográfico eficiente (vide Tabela 2 com o resumo das otimizações implementadas). Ao fim da codificação, o sistema desenvolvido se apresentou capaz de gerar chaves criptográficas, codificar e decodificar mensagens, aos moldes do Sistema McEliece.

Operação:	Implementação da Operação:
Soma em Corpos Finitos	Ou-exclusivo (XOR)
Multiplicação em Corpos Finitos	Consulta a tabelas pré-calculadas
Inverso multiplicativo em Corpos Finitos	Algoritmo de Euclides Estendido
MDC Polinomial	Algoritmo de Euclides Estendido
Teste de Irredutibilidade polinomial	Algoritmo de Ben-Or
Quadrado em Corpos Finitos	“Quadrado de somas é igual à soma dos quadrados” (em corpos finitos de Característica 2)

Tabela 2: Otimizações da Implementação

Conclusões

O Sistema Criptográfico McEliece tem diversas particularidades que o tornam merecedor de estudos mais aprofundados. Sua aplicabilidade, questionada pelo tamanho de suas chaves, deve ser considerada, pois, mesmo sem a evolução da computação quântica, seu uso já é interessante por sua eficiência algorítmica. A implementação deste sistema se mostrou razoavelmente simples quanto à estrutura de dados e complexidade, resumindo a maioria das operações à geração, adição, multiplicação e inversão de matrizes e vetores binários.

Referências Bibliográficas

SHOR, Peter. (1994). “Algorithms for quantum computation: discrete logarithms and factoring”. 35th Annual Symposium on Foundations of Computer. IEEE Comput. Soc. Press.

MCELIECE, Robert. (1978). “A Public-Key Cryptosystem Based On Algebraic Coding Theory”. Deep Space Network Progress Report, 44:114–116.