

Universidade de São Paulo

Criptografia Pós-Quântica com Códigos Corretores de Erros

Rafael Misoczki – IME/USP

misoczki@linux.ime.usp.br

Prof. Dr. Paulo S. L. M. Barreto – Poli/USP

pbarreto@larc.usp.br

Introdução

- O que é Criptografia Pós-Quântica?
- RSA e ECC são vulneráveis a ataques de Computadores Quânticos [Shor 1994]
- Última década: Evolução da Computação Quântica
- Necessidade de solução segura neste contexto
- Alternativa: Criptografia baseada em Códigos Corretores de Erros

Objetivos da Pesquisa

- Compreender, descrever e analisar o sistema criptográfico pós-quântico McEliece e suas derivações (Ex.: CFS)
- Pesquisar maneiras eficientes de implementar as estruturas e operações algébricas necessárias
- Desenvolver uma “Biblioteca Criptográfica Pós-Quântica”
- Escrever artigo para o SBSeg’08

Sistema Criptográfico McEliece

- Sistema de criptografia assimétrica
- Baseado em Códigos Corretores de Erros
- Prós:
 - Não é conhecido algoritmo (seja quântico ou clássico) capaz de quebrá-lo em tempo polinomial
 - Mais eficiente algoritmicamente do que o RSA e ECC
- Contras:
 - Tamanho das chaves
 - Encriptação: 88KB
 - Assinatura Digital: 597KB

Sistema Criptográfico McEliece

■ Geração de Chaves:

- Escolher um código Γ capaz de corrigir até t erros
- Obter a matriz G geradora deste código
- Gerar uma matriz S binária inversível aleatória
- Gerar uma matriz P de permutação aleatória
- Calcular $E = SGP$
- Chave Privada: (S^{-1}, Γ, P^{-1}) Chave Pública: (E, t)

Sistema Criptográfico McEliece

- Encriptação (de mensagem m , com ch. pública: E, t):

- $m' = mE$

- Adicionar vetor e , de peso t , à palavra m' :

$$c = m' + e$$

- Decriptação (de palavra c , com ch. Privada: S^{-1}, Γ, P^{-1}):

- $c' = cP^{-1}$ $(c = mSGP + e \rightarrow c' = mSG + eP^{-1})$

- Tomando eP^{-1} como um erro, corrigir c' obtendo: mSG

- Decodificar mSG em mS

- $m = (mS)S^{-1}$

Sistema de Assinatura Digital (CFS)

- Baseado no Sistema McEliece
- Eficiente algoritmicamente
- Seguro perante computadores quânticos
- Assinatura curta: 81 bits para um esforço de 2^{80} passos computacionais

Implementação

- Biblioteca Criptográfica Pós-Quântica
- Codificada em Linguagem JAVA
- Implementa as otimizações algébricas estudadas
- Capaz de gerar, exportar e importar chaves, além de encriptar e decriptar mensagens
- Representação polinomial de Corpos Finitos binários:
 - Operações módulo um polinômio irredutível
 - Soma: XOR
 - Multiplicação: Consultas a tabelas pré-calculadas
 - “Quadrado de somas é igual à soma dos quadrados”

Implementação

- Teste de Irredutibilidade de Ben-Or
 - mdc
 - mod
 - Endomorfismo de Frobenius
- Estrutura de dados:
 - Vetores e matrizes

Tela inicial



Configurações

Biblioteca Criptográfica Pós-Quântica

Arquivo

Ferramentas

Ajuda

Importar Par de Chaves

Exportar Par de Chaves

Opções

Criptográfica Pós-Quântica

Selecione uma das opções:

Par de Chaves

Encriptação

Deciptação

Sair

O Sistema tem dois parâmetros (m e t) que devem respeitar as seguintes invariantes:

$n = 2^m$

Com 'n' sendo o tamanho do código encriptado

$k = n - m \cdot t > 0$

Com 'k' sendo o tamanho da mensagem original

Selecione uma das opções para os parâmetros:

(Atenção: ao alterá-los, você perderá as chaves carregadas!)

☒ $m = 4, t = 3 \Rightarrow k = 4 \text{ e } n = 16$

☐ $m = 4, t = 2 \Rightarrow k = 8 \text{ e } n = 16$

☐ $m = 5, t = 4 \Rightarrow k = 12 \text{ e } n = 32$

☐ $m = 8, t = 16 \Rightarrow k = 128 \text{ e } n = 256$

Salvar

Nenhuma Par de Chaves selecionado.

Geração de Par de Chaves

Biblioteca Criptográfica Pós-Quântica

Arquivo Ferramentas Ajuda

Biblioteca Criptográfica Pós-Quântica

Selecione uma das opções:

 **Gerar Chaves**

 **Importar Chaves**

 **Exportar Chaves**

 **Voltar**

Digite uma descrição para este Par de Chaves:

Rafael-Keys

Gerar Par de Chaves

Saida:

```
matriz E gerada com sucesso!  
0 1 1 0 1 1 0 1 0 0 1 1 1 0 0 0  
0 0 1 1 0 1 0 1 1 0 0 0 0 0 1 1  
1 0 0 0 1 0 1 0 0 1 1 0 1 1 1 0  
1 0 0 0 0 0 0 1 1 0 1 1 1 1 0 0  
Chave Pública (E, t) gerada com sucesso!  
=====
```

Par de chaves 'Rafael-Keys' gerado com sucesso!

Par de Chaves selecionado: Rafael-Keys

Importação/Exportação de Par de Chaves



Encriptação

Biblioteca Criptográfica Pós-Quântica

Arquivo Ferramentas Ajuda

Biblioteca Criptográfica Pós-Quântica

Selecione uma das opções:

 Par de Chaves

 Encriptação

 Decrptação

 Sair

Par de Chaves selecionado para a Encriptação:

Rafael-Keys

Digite o código binário de 4 bits a ser encriptado:

1010

Criptografar

Mensagem encriptada:

0010011001010110

Saída:

Adicionando 3 erros ao vetor c: 0010011001010110
=====

Mensagem encriptada com sucesso: 0010011001010110

Par de Chaves selecionado: Rafael-Keys

Deciptação

Biblioteca Criptográfica Pós-Quântica

Arquivo Ferramentas Ajuda

Biblioteca Criptográfica Pós-Quântica

Selecione uma das opções:

 Par de Chaves

 Encriptação

 Deciptação

 Sair

Par de Chaves selecionado para a Deciptação:

Rafael-Keys

Digite o código binário de 16 bits a ser deciptado:

0010011001010110

Deciptografar

Mensagem deciptada:

1010

Saída:

Mensagem obtida: 1010

=====

Mensagem deciptada com sucesso!

Par de Chaves selecionado: Rafael-Keys

Conclusão

- Interessante alternativa aos métodos criptográficos tradicionais:
 - Mais eficiente algoritmicamente
 - Seguro (Computação quântica)
- Implementação razoavelmente simples:
 - Em grande parte: manipulações (geração aleatória, adição, multiplicação e inversão) de matrizes e vetores binários



Perguntas?

Rafael Misoczki – IME/USP

`misoczki@linux.ime.usp.br`

<http://linux.ime.usp.br/~misoczki/mac499/>

Referências Bibliográficas

- Shor, P. W. (1994) : “Algorithms for quantum computation: discrete logarithms and factoring”. In Shor, P. W., editor, *35th Annual Symposium on Foundations of Computer Science (Santa Fe, NM, 1994)*, pages 124-134. IEEE Comput. Soc. Press.
- McEliece, R. J. (1978) : “A Public-Key Cryptosystem Based On Algebraic Coding Theory”. *Deep Space Network Progress Report*, 44:114-116.
- Courtois, N., Finiasz, M., and Sendrier, N. (2001): “How to Achieve a McEliece-based Digital Signature Scheme”. In *LNCS*, pages 157-174. Springer Berlin / Heidelberg.

Apêndice I:

McEliece x RSA/ECC

	RSA	ECC	McEliece
Quebra	n^3	n^3	2^n
Operação	n^3	n^3	n^2
Tamanho de chave	1024 bits	160 bits	88 KB

Apêndice II:

Implementação

- Representação de Corpos Finitos (Característica 2):

- Elementos expressos polinomialmente
- Operações módulo polinômio redutor
- Exemplo:
 - Corpo de extensão 4: $g(x) = x^4 + x + 1$
 - Da condição $g(x) = 0$, temos: $x^4 = x + 1$
 - Definimos os demais elementos:

$0 = 0$	$x^4 = x + 1$	$x^8 = x^2 + 1$	$x^{12} = x^3 + x^2 + x + 1$
$x = x$	$x^5 = x^2 + x$	$x^9 = x^3 + x$	$x^{13} = x^3 + x^2 + 1$
$x^2 = x^2$	$x^6 = x^3 + x^2$	$x^{10} = x^2 + x + 1$	$x^{14} = x^3 + 1$
$x^3 = x^3$	$x^7 = x^3 + x + 1$	$x^{11} = x^3 + x^2 + x$	$x^{15} = 1$

- Assim, representação binária (de alguns elementos):

$$x^3 = 1000; \quad x^6 = 1100; \quad x^{11} = 1110; \quad x^{15} = 0001;$$