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"

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 chaves, 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

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?

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 (Shor 1994)	n^3 (Shor 1994)	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:):

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