Criptografia Pós-Quântica baseada em Códigos Corretores de Erros

Gervásio Santos

Instituto de Matemática e Estatísica da USP

gervasio@ime.usp.br

17 de novembro de 2016

Criptografia Atual

- RSA
- Curvas Elípticas

Problema do Logaritmo Discreto

Seja G um grupo. Seja s um elemento de G e g um gerador de G. O **problema do logaritmo discreto** é descobrir $t \in \mathbb{N}$ tal que

$$g^t = s$$

Problema do Logaritmo Discreto

- Difícil em computadores clássicos
- Fácil em computadores quânticos [5]

Criptografia Pós-Quântica

O que fazer quando computadores quânticos se tornarem disponíveis?

- Hashes [4]
- Variáveis Multinomiais [2]
- **Códigos Corretores de Erros** [1, 3]

Códigos Corretores de Erros

- Utilizados em telecomunicações
- Costumam ter estruturas algébricas subjacentes
- **Códigos Lineares**

Códigos Lineares

- Subespaços vetoriais de K^n (K um corpo finito)
- Matrizes geradores
- Matrizes de Teste de Paridade

Criptossistema de McEliece

- **G**: uma matriz k x n, geradora de um código linear de dimensão k.
- ψ: Uma estrutura capaz de corrigir δ erros do código gerado por G.
- **S**: Uma matriz k x k, inversível
- **P**: Uma matriz de permutação n x n

Chaves

O criptossistema de McEliece tem as seguintes chaves pública e privada, respectivamente:

$$K_{\text{pub}} = (\overline{G}, \delta) \quad \text{e} \quad K_{\text{priv}} = (G, \psi, S, P)$$

Onde $\overline{G} = SGP$

Algoritmo de Criptografia

Data: $m \in K^k$, a mensagem a ser criptografada
Result: $c \in K^n$, a mensagem criptografada
Calcule $m' = m\overline{G}$, a palavra do código correspondente a m
Selecione um vetor aleatório $e \in K^n$ de peso δ (o erro)
Calcule $c = m' \oplus e$
return c

Algoritmo de Decriptografia

Data: $c = m\overline{G} \oplus e$, a mensagem criptografada
Result: m, a mensagem original
Calcule $\overline{c} = cP^{-1} = mSG + eP^{-1}$
Use o corretor de erros ψ para remover os erros e obter $\overline{m}$
Resolva o sistema linear sobredeterminado dado por $mSG = \overline{m}$
return m

Códigos de Goppa

Seja K um corpo finito e F uma extensão de K. Tomemos $\varphi(x) \in F[x]$ e $L = \{\alpha_0, \ldots, \alpha_{n-1}\} \subset F$, com $\alpha_i \neq \alpha_j$ se $i \neq j$ e $\varphi(\alpha_k) \neq 0$. Podemos definir o seguinte espaço vetorial sobre K:

$$\Gamma_K(L, \varphi) = \left\{ c \in K^n : \sum_{k=0}^{n-1} c_k (\varphi(\alpha_k))^{-1} \cdot \frac{\varphi(x) - \varphi(\alpha_k)}{x - \alpha_k} = 0 \right\}$$

$\Gamma_K(L, \varphi)$ é chamado de o **Código de Goppa** sobre K com suporte L e polinômio φ.

Um código de Goppa $\Gamma_K(L, \varphi)$ é dito **binário irredutível** se $K = \mathbb{F}_2$ (o corpo de dois elementos), $L \subset \mathbb{F}_{2^m}$ e φ é um polinômio irredutível sobre $F_{2^m}[x]$. Um código de Goppa binário irredutível consegue corrigir $grau(\varphi)$ erros.

Matrizes Diádicas

Dado um corpo K e um vetor $h = (h_1, \ldots, h_n) \in K^n$, a **matriz diádica** $\Delta(h)$ é a matriz simétrica com componentes $\Delta_{ij} = h_{i \oplus j}$.

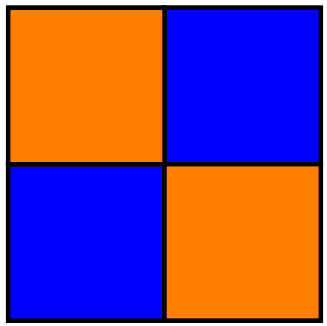

Figura: Matriz diádica

Matriz Quase-Diádica

Uma matriz **quase-diádica** é uma matriz (potencialmente não diádica) de blocos, cujos blocos componentes são matrizes diádicas.

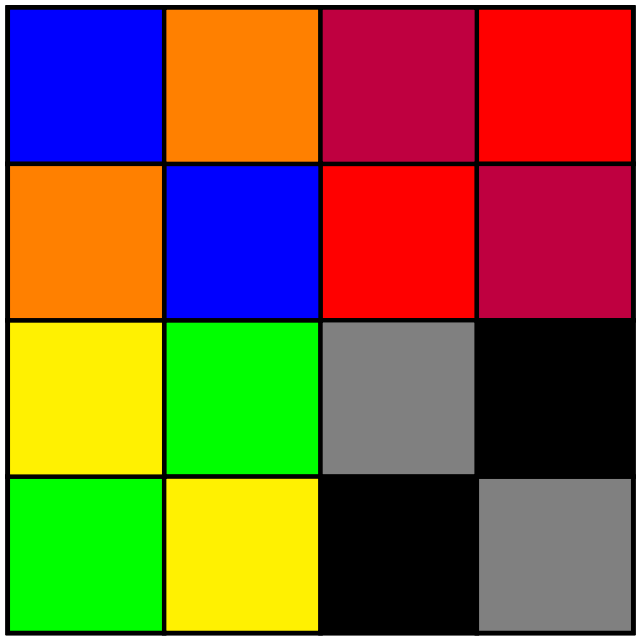

Figura: Matriz quase diádica. Cada bloco 4x4 é uma matriz diádica, bem como cada quadrado colorido.

Códigos de Goppa Quase-Diádicos

- Códigos de Goppa com matriz de teste de paridade quase-diádica
- Permite chaves menores no Criptossistema de McEliece

Códigos MDPC

- *Moderate Density Parity Check*
- Família de códigos cuja matriz de teste de paridade é pouco densa (sem ser totalmente esparsa)
- Desprovidos de estrutura algébrica

Códigos MDPC Quase-Cíclicos

Um código MDPC C de dimensão k sobre $\mathbb{F}_2^n$ é **quase-cíclico** (QC-MDPC) se existe um inteiro η tal que todo shift circular de η bits de uma palavra de C produz outra palavra de C. Particularmente, todas as linhas de uma matriz de teste de paridade de C podem ser obtidas por shifts de η bits da primeira

Comparação

Nível de Segurança	QC-MDPC	QD-Goppa	Goppa Clássico
80	4801	20480	460647
128	9857	32768	1537536
256	32771	65536	7667855

D. Augot, L. Batina, D. J. Bernstein, J. Bos, J. Buchmann, W. Castryck, O. Dunkelman, T. Güneysu, S. Gueron, A. Hülsing, et al.
Initial recommendations of long-term secure post-quantum systems.
Available at pqcrypto.eu.org/docs/initial-recommendations.pdf, 2015.

J. A. Buchmann, L. C. C. García, M. Döring, D. Engelbert, C. Ludwig, R. Overbeck, A. Schmidt, U. Vollmer, and R.-P. Weinmann.
Post-quantum signatures.
IACR Cryptology ePrint Archive, 2004:297, 2004.

R. J. McEliece.
A public-key cryptosystem based on algebraic coding theory.
Deep Space Network Progress Report, 44:114–116, 1978.

R. Merkle.

Security, authentication and public-key systems - A certified digital signature.

PhD thesis, Stanford University, 1979.

P. W. Shor.

Polynomial time algorithms for prime factorization and discrete logarithms on a quantum computer.

SIAM Journal on Computing, 26(5):1481–1509, 1997.