Quatérnios na Criptografia Pós-Quântica

Vitor S. Ponciano [1], Leonardo B. de Souza [2], Rafael Oliveira [1], Augusto Parisot [1] e Everaldo Alves [1]
[1] Centro de Análises de Sistemas Navais- Rio de Janeiro, RJ - Brasil
[2] Centro Federal de Educação Tecnológica Celso Suckow da Fonseca, Rio de Janeiro, RJ- Brasil

***Resumo*— Na era da computação quântica, o paradigma da segurança da informação passa por uma transformação fundamental. Algoritmos criptográficos de chave pública amplamente utilizados, como o RSA, enfrentam uma ameaça existencial. Sua segurança reside na dificuldade computacional de fatorar números inteiros grandes, um problema que o algoritmo de Shor, executado em um computador quântico, consegue resolver eficientemente. Essa vulnerabilidade impulsiona a pesquisa e o desenvolvimento de criptografia pós-quântica (PQC), buscando esquemas criptográficos resistentes a ataques de computadores quânticos. Nesse cenário, o NTRU (Nth Degree Truncated Polynomial Ring Unit) surge como uma solução promissora. Ele se baseia na dificuldade de resolver o problema do vetor mais curto (SVP) em reticulados, um problema que, até o momento, não possui um algoritmo quântico eficiente. Uma extensão inovadora do NTRU é o QTRU, que incorpora a estrutura algébrica dos quatérnios. Este trabalho dedica-se a explorar os fundamentos matemáticos do algoritmo QTRU.**

***Keywords*— Quatérnios, Segurança Pós-Quântica, Computadores Quânticos.**

I. Introdução

A origem da palavra "criptografia " vem da combinação de duas palavras gregas, "kryptós " e "gráphein", que significam respectivamente "oculto"e "escrita", segundo Luciano e Prichett [1]. Baseada em tal estrutura, através dela é possível utilizar uma maneira oculta de representação, com o objetivo de não tornar óbvio o que estava claramente identificado. Quando mencionamos especificamente a segurança virtual, envolve conversão de dados de um formato legível para um formato codificado. Dentro desse contexto, sua eficiência é elemento fundamental na segurança de dados, caracterizando a maneira mais simples e importante de garantir que a informação em um sistema computacional não seja roubada e lida por alguém que deseje usá-la para fins maliciosos.

Destaca-se a chamada criptografia RSA. Nela, as chaves pública e privada são compostas por dois números naturais cada (e, n) e (d, n), respectivamente, onde n é o produto de dois primos, $e * d$, que satisfazem certas relações. Para obter a chave privada a partir da chave pública, basta encontrar a fatoração do número natural n. Nesse contexto, escolhendo convenientemente os dois fatores primos de n, tal fatoração é considerada uma tarefa muito difícil [2].

Desde 1994, com o trabalho do matemático Peter Shor, que introduziu algoritmos quânticos aplicáveis a problemas de fatoração de inteiros e logaritmo discreto [3], tornou-se evidente que o advento dos computadores quânticos poderia potencialmente expor a vulnerabilidade do RSA.

V. Ponciano , ponciano.fundep@marinha.mil.br; L. Souza, oelsouza.math@gmail.com ; A. Pariso, parisot@marinha.mil.br; R. Oliveira, rafael-silva.oliveira@marinha.mil.br; E. Alves, everaldoalves@gmail.com
Este trabalho foi parcialmente financiado pela FINEP, através do Projeto SisCPQDef.

Esquemas criptográficos que resistem a ataques quânticos são conhecidos como *pós-quânticos*. Com o objetivo de acelerar a implementação desses esquemas, o National Institute of Standards and Technology (NIST) iniciou um processo de padronização [4]. Esse processo foca em primitivas essenciais para comunicação segura na Internet, incluindo assinaturas digitais e troca de chaves.

Um dos algoritmos escolhidos pelo NIST foi o sistema criptográfico NTRU (Nth Degree Truncated Polynomial Ring Unit), inspirado em um esquema de criptografia de chave pública (PKE) introduzido por Hoffstein et al [5]. Esquemas de Criptografia de Chave Pública (PKE) são definidos por três algoritmos: geração de chaves, criptografia e descriptografia. Este esquema PKE é baseado em álgebra polinomial e aritmética modular, servindo como base para o sistema criptográfico NTRU. No sistema criptográfico NTRU, a segurança é derivada da dificuldade de resolver o Problema do Vetor Mais Curto (SVP) em reticulados [6].

Uma variante ainda mais robusta do NTRU, é o QTRU, incorpora quatérnios (números hipercomplexos não comutativos) para aumentar a segurança [7]. Sua estrutura matemática complexa dificulta ataques quânticos, mantendo eficiência computacional.

II. Anéis Polinomiais

Um **anel** é um conjunto R equipado com duas operações binárias, adição $(+)$ e multiplicação $(\cdot)$, que satisfazem propriedades específicas:

- **Em relação à Adição $(+)$:** R forma um **grupo abeliano** (comutativo). Isso significa que existe um **elemento neutro aditivo** (0), todo elemento possui um **inverso aditivo**, e a operação é **associativa** e **comutativa**.
- **Em relação à Multiplicação $(\cdot)$:** Existe um **elemento neutro multiplicativo** (1), e a operação é **associativa**. Um anel é considerado **comutativo** se $a \cdot b = b \cdot a$ para todos $a, b \in R$.
- **Propriedade Distributiva:** A multiplicação é **distributiva** sobre a adição, ou seja, $a \cdot (b + c) = a \cdot b + a \cdot c$.

A partir de qualquer anel R, podemos construir um **anel polinomial**, denotado por $R[x]$. Seus elementos são polinômios da forma $a_0 + a_1x + a_2x^2 + \ldots + a_nx^n$, onde os coeficientes a_i pertencem a R. O **grau** de um polinômio não nulo é o maior expoente de x com coeficiente não nulo.

A. Anel Quociente e Aritmética Modular

Uma das ferramentas mais importantes na teoria dos números é a aritmética modular, que envolve o conceito de congruência. Seja R um anel e escolha um elemento não nulo $m \in R$. Dizemos que dois elementos a e b de R são *congruentes módulo* m se a diferença $a - b$ é divisível por

m. Escrevemos $a \equiv b \pmod m$ para indicar que a e b são congruentes módulo m. Por exemplo, 23 é congruente a 2 módulo 7 ($23 = 3*7+2$ *e* $2 = 0*7+2$), significando que 23 e 2 têm o mesmo resto quando divididos por 7.

Seja R um anel e seja $m \in R$ com $m \neq 0$. Para qualquer $a \in R$, escrevemos $\overline{a}$ para o conjunto de todos $a' \in R$ tais que $a' \equiv a \pmod m$. O conjunto $\overline{a}$ é chamado de *classe de congruência* de a, e denotamos a coleção de todas as classes de congruência por $R/(m)$ ou R/mR. Assim, $R/(m) = R/mR = \{\overline{a} : a \in R\}$.

A adição e multiplicação em classes de congruência são dadas por:

$$\overline{a} + \overline{b} = \overline{a+b} \quad \text{e} \quad \overline{a} \cdot \overline{b} = \overline{a \cdot b}. \tag{1}$$

Chamamos $R/(m)$ de anel quociente de R por m. Note que, em $\mathbb{Z}_a$, alguns elementos possuem inversos enquanto outros não. Em geral, se $a \in \mathbb{Z}_q$, então a é invertível se e somente se $\gcd(a, q) = 1$.

Considere como exemplo o anel $F[x]/(x^2+1)$. Cada elemento deste anel quociente é unicamente representado por um polinômio da forma $\alpha + \beta x$, onde $\alpha, \beta \in F$. A adição é realizada como:

$$\overline{\alpha_1 + \beta_1 x + \alpha_2 + \beta_2 x} = \overline{(\alpha_1 + \alpha_2)} + \overline{(\beta_1 + \beta_2)x}. \tag{2}$$

A multiplicação é similar, exceto que precisamos dividir o resultado final por x^2+1 e obter o resto. Assim,

$$\begin{aligned}\overline{(\alpha_1 + \beta_1 x) \cdot (\alpha_2 + \beta_2 x)} &= \overline{\alpha_1\alpha_2 + (\alpha_1\beta_2 + \alpha_2\beta_1)x + \beta_1\beta_2 x^2} \\ &= (\alpha_1\alpha_2 - \beta_1\beta_2) + (\alpha_1\beta_2 + \alpha_2\beta_1)x. \end{aligned}\tag{3}$$

B. Operações em Anéis

Adição de polinômios corresponde à adição vetorial usual:

$$a(x) + b(x) = (a_0 + b_0, a_1 + b_1, a_2 + b_2, \ldots, a_{N-1} + b_{N-1}) \tag{4}$$

O *produto de dois polinômios* $a(x), b(x) \in R$ é dado pela fórmula:

$$a(x) * b(x) = c(x), \text{ onde } c_k = \sum_{i+j \equiv k \pmod N} a_i b_{k-i} \tag{5}$$

onde a soma que define c_k é tomada sobre todos i e j de 0 a $N-1$ que satisfazem a condição $i + j \equiv k \pmod N$. O produto de dois polinômios $a(x), b(x) \in R_q$ é dado pela mesma fórmula, exceto que o valor de c_k é reduzido módulo q.

Vamos calcular o produto $a(x) \cdot b(x)$ no anel $R = \mathbb{Z}[x]/(x^7-1)$, considerando:

$$a(x) = 1 - 2x + 4x^3 \quad \text{e} \quad b(x) = 3 + 4x - 2x^2 \tag{6}$$

Para maior clareza, vamos listar os coeficientes de $a(x)$ e $b(x)$ até a potência $N-1=6$ (preenchendo com zeros os coeficientes inexistentes): $a_0 = 1, a_1 = -2, a_2 = 0, a_3 = 4, a_4 = 0, a_5 = 0, a_6 = 0$ $b_0 = 3, b_1 = 4, b_2 = -2, b_3 = 0, b_4 = 0, b_5 = 0, b_6 = 0$

Usando a fórmula $c_k = \sum_{i+j \equiv k \pmod N} a_i b_{k-i}$, onde $N = 7$, temos:

$$\begin{aligned}
c_0 &= a_0b_0 + a_1b_6 + a_2b_5 + a_3b_4 + a_4b_3 + a_5b_2 + a_6b_1 = 3 \\
c_1 &= a_0b_1 + a_1b_0 + a_2b_6 + a_3b_5 + a_4b_4 + a_5b_3 + a_6b_2 = -2 \\
c_2 &= a_0b_2 + a_1b_1 + a_2b_0 + a_3b_6 + a_4b_5 + a_5b_4 + a_6b_3 = -10 \\
c_3 &= a_0b_3 + a_1b_2 + a_2b_1 + a_3b_0 + a_4b_6 + a_5b_5 + a_6b_4 = 16 \\
c_4 &= a_0b_4 + a_1b_3 + a_2b_2 + a_3b_1 + a_4b_0 + a_5b_6 + a_6b_5 = 16 \\
c_5 &= a_0b_5 + a_1b_4 + a_2b_3 + a_3b_2 + a_4b_1 + a_5b_0 + a_6b_6 = -8 \\
c_6 &= a_0b_6 + a_1b_5 + a_2b_4 + a_3b_3 + a_4b_2 + a_5b_1 + a_6b_0 = 0
\end{aligned}$$

Portanto, no anel $R = \mathbb{Z}[x]/(x^7-1)$, o produto $c(x)$ de $a(x)$ e $b(x)$ é:

$$c(x) = 3 - 2x - 10x^2 + 16x^3 + 16x^4 - 8x^5 \quad \text{em} \quad R = \mathbb{Z}[x]/(x^7-1)$$

Os coeficientes módulo um número primo, por exemplo 5, teríamos:

$$\begin{aligned}
&c_0 \equiv 3 \pmod 5,\ c_1 \equiv -2 \equiv 3 \pmod 5 \\
&c_2 \equiv -10 \equiv 0 \pmod 5,\ c_3 \equiv 16 \equiv 1 \pmod 5 \\
&c_4 \equiv 16 \equiv 1 \pmod 5,\ c_5 \equiv -8 \equiv 2 \pmod 5 \\
&c_6 \equiv 0 \pmod 5
\end{aligned}$$

Portanto, em $(\mathbb{Z}/5\mathbb{Z})[x]/(x^7-1)$, o produto $c(x)$ é:

$$c(x) = 3 + 3x + x^3 + x^4 + 2x^5 \quad \text{em} \quad (\mathbb{Z}/5\mathbb{Z})[x]/(x^7-1)$$

C. Inverso em R_q

Seja q um número primo. Então, $a(x) \in R_q$ possui inverso multiplicativo se, e somente se,

$$\gcd(a(x), x^N - 1) = 1 \quad \text{em } (\mathbb{Z}/q\mathbb{Z})[x].$$

A operação gcd significa *máximo divisor comum* (greatest common divisor). O inverso $a(x)^{-1} \in R_q$ pode ser calculado utilizando o algoritmo estendido de Euclides. Ou seja, encontra-se polinômios $u(x)$ e $v(x)$ em $(\mathbb{Z}/q\mathbb{Z})[x]$ que satisfazem

$$a(x)u(x) + (x^N - 1)v(x) = 1.$$

Então, $a(x)^{-1} = u(x)$ em R_q.

Sejam $N = 5$ e $q = 2$. Vamos calcular $(1 + x + x^4)^{-1}$ em R_2. Note que, em $\mathbb{Z}_2$, temos $1 - x^5 = 1 + x^5$.

Aplicamos o algoritmo de Euclides a $1 + x + x^4$ e $1 + x^5$ em $(\mathbb{Z}/2\mathbb{Z})[x]$.

Passo 1. Efetuamos a primeira divisão:

$$x^5 + 1 = x \cdot (x^4 + x + 1) + (x^2 + x + 1).$$

Passo 2. Dividimos $x^4 + x + 1$ pelo resto $x^2 + x + 1$:

$$x^4 + x + 1 = (x^2 + x) \cdot (x^2 + x + 1) + 1.$$

Como o resto é 1, concluímos que $\gcd(1+x+x^4, x^5+1) = 1$.

Passo 3. Retrocedemos pelas contas (usando o método de substituição) para expressar 1 como combinação de $1+x+x^4$ e x^5+1. A retro-substituição resulta em:

$$1 = (x^4 + x + 1) + (x^2 + x)(x^2 + x + 1)$$

e, observando que

$$(x^2+x)(x^2+x+1) = x^5+1+x(x^4+x+1),$$

obtemos:

$$1 = (x^4+x+1)(x^3+x^2+1) + (x^5+1)(x^2+x).$$

Dessa forma, no anel R_2 temos:

$$(1+x+x^4)(x^3+x^2+1) \equiv 1 \pmod{x^5+1}.$$

Conclusão: O inverso multiplicativo de $1+x+x^4$ em R_2 é

$$(1+x+x^4)^{-1} = 1+x^2+x^3.$$

III. NTRU-HRSS

Nesta seção, descrevemos o NTRU. Começamos fixando um inteiro $N \geq 1$ e dois módulos p e q. Definimos os anéis de convolução de polinômios R, R_p e R_q como segue: Começamos fixando um inteiro $N \geq 1$ e dois módulos p e q, e sejam R, R_p e R_q os anéis de convolução de polinômios:

$$R = \mathbb{Z}[x]/(x^N-1) \tag{7}$$

$$R_p = (\mathbb{Z}/p\mathbb{Z})[x]/(x^N-1) \quad \text{e} \quad R_q = (\mathbb{Z}/q\mathbb{Z})[x]/(x^N-1) \tag{8}$$

Podemos ver um polinômio $R[x] \in R$ como um elemento de R_p ou R_q reduzindo seus coeficientes módulo p ou q. Inversamente, usamos levantamentos centrais para mover elementos de R_p ou R_q para R.

A. Polinômios Ternários

Definição. Para quaisquer inteiros positivos d_1 e d_2, denotamos por $T(d_1, d_2)$ o conjunto:

$$T(d_1,d_2) = \{a(x) \in R\} = \begin{cases} d_1 & \text{coeficientes iguais a 1,} \\ d_2 & \text{coeficientes iguais a -1} \\ & \text{outros coeficientes iguais a 0} \end{cases}$$

IV. Criação de Parâmetros Públicos

Agora estamos prontos para descrever o NTRU. Alice (ou alguma autoridade confiável) escolhe parâmetros públicos (N, q) que satisfazem as diretrizes descritas anteriormente. A chave privada de Alice consiste em dois polinômios escolhidos aleatoriamente com $d = \frac{q}{8} - 2$:

$$f(x) \in T(d+1, d) \quad \text{e} \quad g(x) \in T(d,d). \tag{9}$$

Alice calcula as inversas:

$$F_q(x) = f(x)^{-1} \text{ em } R_q \quad \text{e} \quad F_p(x) = f(x)^{-1} \text{em } R_p. \tag{10}$$

Se alguma das inversas não existir, Alice descarta esse $f(x)$ e escolhe um novo. Vale mencionar que Alice escolhe $f(x)$ de $T(d+1, d)$, em vez de $T(d,d)$, porque elementos em $T(d,d)$ nunca têm inversas em R_q.

Em seguida, Alice calcula

$$h(x) = F_q(x) * g(x) \quad \text{em} \quad R_q. \tag{11}$$

O polinômio $h(x)$ é a chave pública de Alice. Sua chave privada, da qual ela precisará para descriptografar mensagens, é o par $(f(x), F_q(x))$ ou $(f(x), F_p(x))$

A. Criptografia

O texto plano de Bob é um polinômio $m(x) \in R$ cujos coeficientes satisfazem $-p/2 < m_i \leq p/2$, ou seja, o texto plano m é um polinômio em R que é o levantamento central de um polinômio em R_p. Bob escolhe um polinômio aleatório (um elemento aleatório) $r(x) \in T(d,d)$ e calcula

$$e(x) \equiv ph(x) * r(x) + m(x) \pmod{q}. \tag{12}$$

O texto cifrado de Bob, $e(x)$, está no anel R_q.

B. Descriptografia

Ao receber o texto cifrado de Bob, Alice inicia o processo de decriptografia calculando

$$a(x) \equiv f(x) * e(x) \pmod{q}. \tag{13}$$

Ela então aplica o levantamento central a $a(x)$ para obter um elemento em R, e realiza um cálculo módulo p,

$$b(x) \equiv F_p(x) * a(x) \pmod{p}. \tag{14}$$

Assumindo que os parâmetros foram escolhidos corretamente, agora verificamos que o polinômio $b(x)$ é igual ao texto plano $m(x)$.

Quando Alice calcula $a(x)$ módulo q (ou seja, em R_q) e então aplica o levantamento central para R, ela recupera o valor exato. Em outras palavras,

$$a(x) = pg(x) * r(x) + f(x) * m(x) \tag{15}$$

exatamente em R, não apenas módulo q.

Alice multiplica $a(x)$ por $F_p(x)$, a inversa de $f(x)$ módulo p, e reduz o resultado módulo p para obter

$$\begin{aligned} b(x) &\equiv F_p(x) * a(x) \pmod{p} \equiv \\ & F_p(x) * (pg(x) * r(x) + f(x) * m(x)) \pmod{p} \\ &\equiv F_p(x) * f(x) * m(x) \pmod{p} \equiv m(x) \pmod{p} \end{aligned} \tag{16}$$

Portanto, $b(x)$ e $m(x)$ são iguais módulo p.

C. Exemplo de Uso do NTRU

Geração de Parâmetros Públicos:

- Escolha parâmetros públicos (N, p, q, d) onde N e p são primos, $\gcd(p, q) = \gcd(N, q) = 1$, e $q > (6d+1)p$.

Geração de Chaves:

- Escolha $f \in T(d+1, d)$ invertível em R_q e R_p.
- Escolha $g \in T(d, d)$.
- Calcule F_q, a inversa de f em R_q.
- Calcule F_p, a inversa de f em R_p.
- Publique a chave pública $h = F_q \otimes g$.

Criptografia: $\{m, h\}$

- Escolha um texto plano $m \in R_p$.
- Escolha um valor aleatório $r \in T(d,d)$.
- Calcule $e \equiv pr \otimes h + m \pmod{q}$.
- **retorne** e.

Decriptografia: $\{e, f\}$

- Calcule $f \otimes e \equiv pg \otimes r + f \otimes m \pmod{q}$.
- Levante ao centro para $a \in R$ e calcule $m \equiv F_p \otimes a \pmod{p}$.

- **retorne** m.

Apresentamos um pequeno exemplo numérico de NTRU com parâmetros públicos. Para este exemplo, usamos os seguintes parâmetros públicos: $N = 17$, $p = 3$, $q = 16$, $d = 8$.

Chave Privada de Alice: A chave privada de Alice consiste em dois polinômios escolhidos aleatoriamente:

$$f(x) = -x^5 + x^2 + x,\ g(x) = x^{16} + x^{13} - x^5. \tag{17}$$

Cálculo das Inversas: Para calcular as inversas, Alice usa as seguintes fórmulas:

$$\begin{aligned} F_p(x) &= f(x)^{-1} \mod p \\ &= x^{15} - x^{14} - x^{10} - x^7 - x^6 - x^4 + x^3 - x^2 - x, \\ F_q(x) &= f(x)^{-1} \mod q \\ &= -6x^{16} + x^{15} + 2x^{14} + x^{13} - 6x^{12} \\ &+ 3x^{11} + 3x^{10} - 5x^9 - 3x^8 \\ &+ 6x^7 - 2x^6 + 8x^5 + 3x^4 + 4x^3 + 6x^2 - 5x + 7. \end{aligned}$$

Alice armazena $f(x)$ e $F_p(x)$ como sua chave privada e calcula sua chave pública, $h(x)$, e a publica. A chave pública é dada por:

$$\begin{aligned} h(x) &= F_q(x) \cdot g(x) \\ &= 8x^{16} - 3x^{15} + x^{14} - 4x^{13} + 5x^{12} \\ &- 3x^{11} - 3x^{10} + x^9 + x^8 \\ &- 6x^7 - 2x^6 + 2x^5 - 5x^4 + 8x^3 - 3x + 4. \end{aligned}$$

Texto Cifrado de Bob: Bob calcula e envia para Alice o texto cifrado $e(x)$:

$$\begin{aligned} e(x) &= pr(x) * h(x) + m(x) \\ &= -7x^{16} - 6x^{15} - 7x^{14} + 2x^{13} \\ &+ 5x^{12} - 2x^{10} + 5x^9 + 4x^8 \\ &- 5x^7 - x^5 + 8x^4 - 5x^3 - 2x^2 + 6x + 6. \end{aligned}$$

Decriptografia de Alice: Para decodificar a mensagem de Bob, Alice usa a seguinte operação: $m(x) = -x^{12} + x^8 + x^5$

V. Álgebra dos Quatérnios

A álgebra dos quatérnios, foi definidas por William Rowan Hamilton em 1843, forma um espaço vetorial de 4 dimensões sobre $\mathbb{R}$. Os elementos da álgebra dos quatérnios $\mathbb{H}$ são expressos como:

$$\mathbb{H} = \{\alpha + \beta i + \gamma j + \delta k \mid \alpha, \beta, \gamma, \delta \in \mathbb{R}\} \tag{18}$$

com as regras de multiplicação:

$$\begin{aligned} &i^2 = j^2 = k^2 = -1,\ ij = -ji = k,\ jk = -kj = i, \\ &ki = -ik = j \end{aligned}$$

Regras de adição para dois quatérnios:

$$q = \langle \alpha, \beta, \gamma, \delta \rangle \quad \text{e} \quad q' = \langle \alpha', \beta', \gamma', \delta' \rangle :$$

$$q + q' = \langle \alpha + \alpha', \beta + \beta', \gamma + \gamma', \delta + \delta' \rangle \tag{19}$$

A. Multiplicação de Quatérnios via Matrizes em $\mathbb{R}^4$

Vamos calcular o produto de dois quatérnios, q e q', utilizando a representação matricial em $\mathbb{R}^4$.

Sejam os quatérnios:

$$q = 2 - i + 5j - k \quad \text{e} \quad q' = -1 + 3i - 2j + 4k.$$

Um quatérnio $q = a + bi + cj + dk$ pode ser representado como uma **matriz de multiplicação à esquerda** $\mathbf{L}_q \in \mathbb{R}^{4\times4}$:

$$\mathbf{L}_q = \begin{bmatrix} a & -b & -c & -d \\ b & a & -d & c \\ c & d & a & -b \\ d & -c & b & a \end{bmatrix}$$

Para $q = 2 - i + 5j - k$:

$$\begin{aligned} \mathbf{L}_{2-i+5j-k} &= \begin{bmatrix} 2 & -(-1) & -5 & -(-1) \\ -1 & 2 & -(-1) & 5 \\ 5 & -1 & 2 & -(-1) \\ -1 & -5 & -1 & 2 \end{bmatrix} \\ &= \begin{bmatrix} 2 & 1 & -5 & 1 \\ -1 & 2 & 1 & 5 \\ 5 & -1 & 2 & 1 \\ 1 & -5 & -1 & 2 \end{bmatrix} \end{aligned}$$

O quatérnio q' é tratado como um **vetor em** $\mathbb{R}^4$:

$$\mathbf{v}_{q'}^T = \begin{bmatrix} -1 & 3 & -2 & 4 \end{bmatrix}$$

Para calcular qq', multiplicamos a matriz $\mathbf{L}_q$ pelo vetor $\mathbf{v}_{q'}$:

$$\mathbf{L}_q \mathbf{v}_{q'} = \begin{bmatrix} 2 & 1 & -5 & 1 \\ -1 & 2 & 1 & 5 \\ 5 & -1 & 2 & 1 \\ 1 & -5 & -1 & 2 \end{bmatrix} \begin{bmatrix} -1 \\ 3 \\ -2 \\ 4 \end{bmatrix} = \begin{bmatrix} 15 \\ 25 \\ -8 \\ -6 \end{bmatrix}$$

Assim, $qq' = 15 + 25i - 8j - 6k$.

Para ilustrar a não-comutatividade dos quatérnios, vamos calcular também $q'q$. Primeiro, a matriz $\mathbf{L}_{q'}$ para $q' = -1 + 3i - 2j + 4k$:

$$\mathbf{L}_{q'} = \begin{bmatrix} -1 & -3 & -(-2) & -4 \\ 3 & -1 & -4 & -2 \\ -2 & 4 & -1 & -3 \\ 4 & -(-2) & 3 & -1 \end{bmatrix} = \begin{bmatrix} -1 & -3 & 2 & -4 \\ 3 & -1 & -4 & -2 \\ -2 & 4 & -1 & -3 \\ 4 & 2 & 3 & -1 \end{bmatrix}$$

E o vetor $\mathbf{v}_q$ para $q = 2 - i + 5j - k$:

$$\mathbf{v}_q^T = \begin{bmatrix} 2 & -1 & 5 & -1 \end{bmatrix}$$

Agora, calculamos $\mathbf{L}_{q'} \mathbf{v}_q$:

$$\mathbf{L}_{q'} \mathbf{v}_q = \begin{bmatrix} -1 & -3 & 2 & -4 \\ 3 & -1 & -4 & -2 \\ -2 & 4 & -1 & -3 \\ 4 & 2 & 3 & -1 \end{bmatrix} \begin{bmatrix} 2 \\ -1 \\ 5 \\ -1 \end{bmatrix} = \begin{bmatrix} 15 \\ -11 \\ -10 \\ 22 \end{bmatrix}$$

Assim, $q'q = 15 - 11i - 10j + 22k$.

Como esperado, os resultados são diferentes, o que demonstra a **não-comutatividade** da multiplicação de quatérnios:

$$\boxed{qq' = 15 + 25i - 8j - 6k \neq q'q = 15 - 11i - 10j + 22k}$$

B. Propriedades Importantes dos Quatérnios

Para um quatérnio $q = \alpha + \beta i + \gamma j + \delta k$, definimos as seguintes propriedades:

- **Conjugado ($\bar{q}$)**: O conjugado de q é obtido invertendo o sinal das partes imaginárias: $\bar{q} = \alpha - \beta i - \gamma j - \delta k$
- **Norma ($N(q)$)**: A norma de um quatérnio é o produto de q pelo seu conjugado, resultando em um número real que é a soma dos quadrados de seus coeficientes:

$$N(q) = q\bar{q} = \alpha^2 + \beta^2 + \gamma^2 + \delta^2$$

- **Inversa (q^{-1})**: A inversa de um quatérnio q (quando sua norma não é zero) é o seu conjugado dividido pela sua norma. É análogo ao inverso de um número complexo:

$$q^{-1} = \frac{\bar{q}}{N(q)}, \quad \text{quando } N(q) \neq 0$$

—

1) Exemplo de Cálculo de Inversa: Vamos calcular a inversa do quatérnio $q = 2 - i + 3j - 4k$.

1) **Encontre o Conjugado de** q:

$$\bar{q} = 2 - (-1)i - 3j - (-4)k = 2 + i - 3j + 4k$$

2) **Calcule a Norma de** q:

$$N(q) = (2)^2+(-1)^2+(3)^2+(-4)^2 = 4+1+9+16 = 30$$

3) **Calcule a Inversa de** q:

$$q^{-1} = \frac{\bar{q}}{N(q)} = \frac{2 + i - 3j + 4k}{30}$$

VI. Estrutura Algébrica do QTRU

O criptossistema QTRU fundamenta-se em álgebras de quatérnios definidas sobre anéis quocientes de polinômios [7]. Em particular, são considerados os anéis:

$$A_0 = \left(\frac{-1,-1}{\mathbb{Z}_p[x]/(x^N-1)}\right), A_1 = \left(\frac{-1,-1}{\mathbb{Z}_q[x]/(x^N-1)}\right) \quad (20)$$

Essas estruturas representam extensões dos quatérnios de Hamilton onde os coeficientes pertencem ao anel quociente $\mathbb{Z}_p[x]/(x^N - 1)$. Elementos de A_0 e A_1 são expressos na forma:

$$q = a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}, \quad \text{com } a, b, c, d \in \mathbb{Z}_p[x]/(x^N - 1)$$

As unidades $\mathbf{i}, \mathbf{j}, \mathbf{k}$ obedecem às relações:

$$\mathbf{i}^2 = \mathbf{j}^2 = -1, \quad \mathbf{ij} = \mathbf{k}, \quad \mathbf{ji} = -\mathbf{k}$$

Exemplo Numérico

Considere o quatérnio polinomial $q_3 \in \left(\frac{-1,-1}{\mathbb{Z}_5[x]/(x^3-1)}\right)$ definido por: $q_3 = 1 + \mathbf{i} + \mathbf{j} + \mathbf{k}$

Aqui, $N = 3$ e estamos trabalhando com coeficientes em $\mathbb{Z}_5$.

Passo 1: Cálculo da Norma $N(q_3)$: A norma de um quatérnio $q = a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$ é dada por:

$$N(q) = a^2 + b^2 + c^2 + d^2$$

Para $q_3 = 1 + \mathbf{i} + \mathbf{j} + \mathbf{k}$, seus coeficientes são $a = 1, b = 1, c = 1, d = 1$. Calculando a norma em $\mathbb{Z}_5[x]/(x^3 - 1)$:

$$N(q_3) = (1)^2 + (1)^2 + (1)^2 + (1)^2 = 4$$

Portanto, $N(q_3) = 4$ em $\mathbb{Z}_5[x]/(x^3 - 1)$.

Passo 2: Inverso da Norma $N(q_3)^{-1}$: Para encontrar o inverso de $N(q_3) = 4$ no anel $\mathbb{Z}_5[x]/(x^3 - 1)$, que é um anel com coeficientes em $\mathbb{Z}_5$, buscamos o inverso de 4 em $\mathbb{Z}_5$.

Sabemos que $4 \cdot 4 = 16 \equiv 1 \pmod 5$. Assim, o inverso multiplicativo de 4 em $\mathbb{Z}_5$ é 4.

Portanto, $N(q_3)^{-1} = 4$.

Passo 3: Cálculo do Inverso q_3^{-1}: O inverso de um quatérnio q é dado por:$q^{-1} = N(q)^{-1} \cdot \overline{q}$

onde $\overline{q} = a - b\mathbf{i} - c\mathbf{j} - d\mathbf{k}$ é o conjugado de q.

Para $q_3 = 1 + \mathbf{i} + \mathbf{j} + \mathbf{k}$, o conjugado é:$\overline{q_3} = 1 - \mathbf{i} - \mathbf{j} - \mathbf{k}$ Finalmente, o inverso de q_3 é:

$$q_3^{-1} = N(q_3)^{-1} \cdot \overline{q_3} = 4 \cdot (1 - \mathbf{i} - \mathbf{j} - \mathbf{k}) = 4 - 4\mathbf{i} - 4\mathbf{j} - 4\mathbf{k}$$

A. Esquema Proposto: QTRU

Semelhante ao NTRU, a segurança do criptossistema QTRU depende de três parâmetros (N, p, q) e de quatro subconjuntos $L_f, L_m, L_\phi, L_g \subset A$, onde:

$$A_q = \left(\frac{-1,-1}{\mathbb{Z}_p[x]/(x^N-1)}\right), A_p = \left(\frac{-1,-1}{\mathbb{Z}_q[x]/(x^N-1)}\right) \quad (21)$$

Aqui, N, p e q são constantes que exercem funções análogas aos parâmetros equivalentes no NTRU. As constantes d_f, d_g, d_ϕ e d_m, bem como os subconjuntos L_f, L_ϕ, L_g e L_m, seguem a mesma definição.

Exemplo de Uso do Criptossistema QTRU

Neste exemplo, usaremos os parâmetros: $N = 3$, $p = 5$, $q = 13$, e $d = 1$. Trabalharemos com polinômios nos anéis $\mathbb{Z}_p[x]/(x^3 - 1)$ e $\mathbb{Z}_q[x]/(x^3 - 1)$. Para simplificar, focaremos nos **componentes escalares** (ou seja, quatérnios com apenas a parte real não nula).

a) Geração de Chaves:: Alice escolhe dois polinômios, $\tilde{F}$ e $\tilde{G}$.

- Escolha $\tilde{F} = f_0 + 0i + 0j + 0k$, onde $f_0 \in \mathbb{Z}[x]/(x^3 - 1)$. Por exemplo, $f_0(x) = 1 + x$.
- Escolha $\tilde{G} = g_0 + 0i + 0j + 0k$, onde $g_0 \in \mathbb{Z}[x]/(x^3 - 1)$. Por exemplo, $g_0(x) = x^2 - x$.

Calculamos as inversas de $\tilde{F}$ nos anéis.

- **Inversa de $\tilde{F}$ em $A_q = \mathbb{Z}_{13}[x]/(x^3 - 1)$ ($\tilde{F}_q$):** $f_0(x) = 1 + x$. Precisamos encontrar $(1 + x)^{-1} \pmod{13}$ em $\mathbb{Z}_{13}[x]/(x^3 - 1)$. Como $(x+1)(x^2 - x + 1) = x^3 + 1 \equiv 1 + 1 = 2 \pmod{x^3 - 1}$, e o inverso de 2 em $\mathbb{Z}_{13}$ é 7 (pois $2 \cdot 7 = 14 \equiv 1 \pmod{13}$), então $(1 + x)^{-1} = 7(x^2 - x + 1) = 7x^2 - 7x + 7 \pmod{13}$. Portanto, $\tilde{F}_q = (7x^2 + 6x + 7) + 0i + 0j + 0k$.
- **Inversa de $\tilde{F}$ em $A_p = \mathbb{Z}_5[x]/(x^3 - 1)$ ($\tilde{F}_p$):** $f_0(x) = 1 + x$. Precisamos encontrar $(1 + x)^{-1} \pmod 5$ em

$\mathbb{Z}_5[x]/(x^3-1)$. Novamente, $(x+1)(x^2-x+1) = x^3+1 \equiv 1+1 = 2 \pmod{x^3-1}$. Em $\mathbb{Z}_5$, a inversa de 2 é 3. Então, $(1+x)^{-1} = 3(x^2-x+1) = 3x^2-3x+3 = 3x^2+2x+3 \pmod 5$. Portanto, $\tilde{F}_p = (3x^2+2x+3)+0i+0j+0k$.

A **chave pública** de Alice é $\tilde{H} = \tilde{F}_q \circ \tilde{G}$. Para os componentes escalares: $h_0(x) = f_{q,0}(x) \cdot g_0(x)$.

$$\begin{aligned}
h_0(x) &= (7x^2+6x+7)\cdot(x^2-x) \pmod{13} \\
&= 7x^4-7x^3+6x^3-6x^2+7x^2-7x \\
&\equiv 7x-7+6-6x^2+7x^2-7x \pmod{x^3-1,13} \\
&\equiv (7-7)x^4+(-7+6)x^3 \\
&+(-6+7)x^2+(7-7)x+(-7+6) \\
&\equiv (7x^2+6x+7)(x^2-x) \\
&= 7x^4-7x^3+6x^3-6x^2+7x^2-7x \\
&\equiv 7x-7+6-6x^2+7x^2-7x \pmod{x^3-1,13} \\
&\equiv (7-7)x+(-7+6)+(-6+7)x^2 \\
&\equiv 0x+(-1)+x^2 \pmod{13} \\
&\equiv x^2-1 \pmod{13} \equiv x^2+12 \pmod{13}
\end{aligned}$$

Portanto, a chave pública é $\tilde{H} = (x^2+12)+0i+0j+0k$.

b) Criptografia (Bob): Bob quer criptografar uma mensagem $\tilde{M}$.

- Mensagem $\tilde{M} = m_0+0i+0j+0k$, com $m_0 \in \mathbb{Z}_5[x]/(x^3-1)$ tendo coeficientes no intervalo $(-p/2, p/2]$. Por exemplo, $m_0(x) = 1+x$.
- Geração de um polinômio aleatório $\tilde{\Phi} = \phi_0+0i+0j+0k$. Por exemplo, $\phi_0(x) = x^2-1$.

Bob calcula o texto cifrado $\tilde{E} \equiv p\tilde{\Phi} \circ \tilde{H} + \tilde{M} \pmod q$. Para os componentes escalares: $e_0(x) \equiv p \cdot \phi_0(x) \cdot h_0(x) + m_0(x) \pmod{13}$.

$$\begin{aligned}
&p\cdot\phi_0(x)\cdot h_0(x) = 5\cdot(x^2-1)\cdot(x^2+12) \pmod{13} \\
&= 5\cdot(x^4+12x^2-x^2-12) \pmod{13} \\
&\equiv 5\cdot(x+11x^2-12) \pmod{13} \\
&\equiv 5x+55x^2-60 \pmod{13} \\
&\equiv 5x+3x^2-8 \pmod{13} \equiv 3x^2+5x+5 \pmod{13}
\end{aligned}$$

Agora, adicionamos a mensagem:

$$\begin{aligned}
e_0(x) &\equiv (3x^2+5x+5)+(1+x) \pmod{13} \\
&\equiv 3x^2+6x+6 \pmod{13}
\end{aligned}$$

O texto cifrado é $\tilde{E} = (3x^2+6x+6)+0i+0j+0k$.

c) Decriptografia (Alice): Alice recebe $\tilde{E}$ e usa sua chave privada $\tilde{F}$.

- Calcula $\tilde{A} \equiv \tilde{F} \circ \tilde{E} \pmod q$. Para os componentes escalares: $a_0(x) \equiv f_0(x) \cdot e_0(x) \pmod{13}$.

$$\begin{aligned}
a_0(x) &\equiv (1+x)\cdot(3x^2+6x+6) \pmod{13} \\
&\equiv 3x^2+6x+6+3x^3+6x^2+6x \pmod{13} \\
&\equiv 3x^2+6x+6+3+6x^2+6x \pmod{x^3-1,13} \\
&\equiv (6+3)+(6+6)x+(3+6)x^2 \pmod{13} \\
&\equiv 9+12x+9x^2 \pmod{13}
\end{aligned}$$

  Portanto, $\tilde{A} = (9+12x+9x^2)+0i+0j+0k$.
- Centraliza os coeficientes de $\tilde{A}$ no intervalo $(-q/2, q/2]$. Neste caso, $q=13$, então o intervalo é $(-6.5, 6.5]$. $9 \equiv -4 \pmod{13}$ $12 \equiv -1 \pmod{13}$ $9 \equiv -4 \pmod{13}$ Então, $\tilde{A}_{\text{centralizado}} = (-4-x-4x^2)+0i+0j+0k$.
- Calcula $\tilde{M}' \equiv \tilde{F}_p \circ \tilde{A}_{\text{centralizado}} \pmod p$. Para os componentes escalares: $m'_0(x) \equiv f_{p,0}(x) \cdot a_{0,\text{centralizado}}(x) \pmod 5$. Lembre-se que $f_{p,0}(x) = 3x^2+2x+3$. Reduzindo $a_{0,\text{centralizado}}(x)$ módulo 5: $-4-x-4x^2 \equiv 1-x-4x^2 \equiv 1+4x+x^2 \pmod 5$.

$$\begin{aligned}
m'_0(x) &\equiv (3x^2+2x+3)\cdot(1+4x+x^2) \pmod 5 \\
&\equiv 3x^2+12x+3x^3+2x+8x^2+2x^3 \\
&+3+12x+3x^2 \pmod 5 \\
&\equiv 3x^2+2x+3+3+2x+3x^2 \\
&+3+2x^2+2+3x^2+2x+3 \pmod{x^3-1,5} \\
&\equiv (3+3+2+3)+(2+2+2)x \\
&+(3+3+2+3)x^2 \pmod 5 \\
&\equiv 11+6x+11x^2 \pmod 5 \\
&\equiv 1+x+x^2 \pmod 5
\end{aligned}$$

VII. Conclusão

A natureza não comutativa da álgebra dos quatérnios confere ao criptossistema QTRU uma robustez inerente contra ataques baseados em reticulados (lattice-based attacks). O QTRU explora a sofisticada estrutura algébrica dos quatérnios para potencialmente oferecer um nível de segurança superior ao do NTRU tradicional. A não comutatividade da multiplicação quaterniônica, aliada à sua estrutura de dimensão superior, torna o sistema mais resistente a diversas técnicas de criptoanálise conhecidas, sem comprometer de forma proibitiva a eficiência computacional. Assim, o QTRU emerge como uma alternativa promissora no campo da criptografia pós-quântica, merecendo investigação e análise contínuas para a compreensão completa de suas propriedades de segurança e desempenho.

Referências

[1] D. Luciano and G. Prichett, "Cryptology: From caesar ciphers to public-key cryptosystems," *The College Mathematics Journal*, 1987.

[2] S. C. Coutinho, *The Mathematics of Ciphers: Number Theory and RSA Cryptography*. AK Peters/CRC Press, 1999.

[3] P. W. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," in *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*. IEEE, 1994, pp. 124–134.

[4] L. Chen *et al.*, "Report on post-quantum cryptography," US Department of Commerce, National Institute of Standards and Technology, Tech. Rep., 2016.

[5] J. Hoffstein, J. Pipher, and J. H. Silverman, "Ntru: A ring-based public key cryptosystem," in *International Algorithmic Number Theory Symposium*. Springer, 1998, pp. 267–288.

[6] J. H. Silverman *et al.*, *An Introduction to Mathematical Cryptography*. Springer, 2008, vol. 1.

[7] E. Malekian, A. Zakerolhsooeini, and A. Mashatan, "Qtru: Quaternion version of the ntru public-key cryptosystems," *The ISC International Journal of Information Security*, vol. 3, pp. 29–42, 2011.