Álgebra polinomial e Aritmética modular em criptografia aplicada ao NTRU na era da computação quântica.

Vitor Ponciano, Vilc Rufino-CASNAV-Marinha

July 2, 2024

Introdução

- A criptografia desempenha um papel crucial na proteção de informações sensíveis, mas com o avanço da computação quântica, muitos dos algoritmos criptográficos convencionais podem se tornar vulneráveis.

Figure: Criptografia

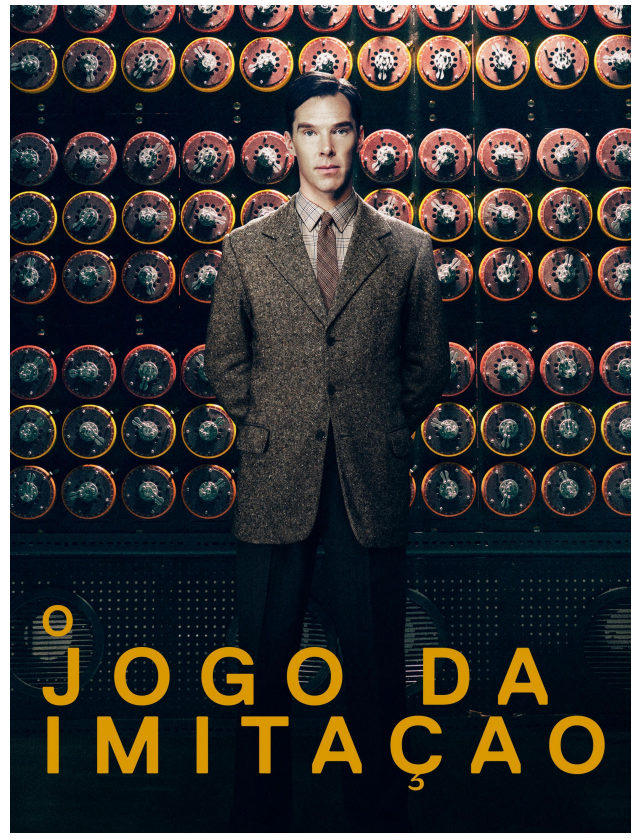

Figure: Jogo de Imitação

Introdução

- Uma solução promissora é o NTRU, que se baseia em problemas matemáticos envolvendo anéis polinomiais e aritmética modular para resistir a ataques de computadores quânticos.

Figure: Algoritmos quânticos

- Desde 1994, com a introdução dos algoritmos quânticos por Peter Shor, ficou claro que os computadores quânticos poderiam expor a vulnerabilidade de sistemas criptográficos convencionais como criptografia RSA, por exemplo, depende da fatoração de números inteiros para garantir segurança.

Anel

Um anel é um conjunto R que possui duas operações, denotadas por $+$ e $\cdot$, que satisfazem as seguintes propriedades:
Propriedades de $+$:

- **Lei da Identidade:** Existe um elemento identidade aditivo $0 \in R$ tal que $0 + a = a + 0 = a$ para todo $a \in R$.
- **Lei do Inverso:** Para todo elemento $a \in R$, existe um inverso aditivo $b \in R$ tal que $a + b = b + a = 0$.
- **Lei Associativa:** $a + (b + c) = (a + b) + c$ para todo $a, b, c \in R$.
- **Lei Comutativa:** $a + b = b + a$ para todo $a, b \in R$.

Anel

Propriedades de $\cdot$:

- **Lei da Identidade:** Existe um elemento identidade multiplicativo $1 \in R$ tal que $1 \cdot a = a \cdot 1 = a$ para todo $a \in R$.
- **Lei Associativa:** $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ para todo $a, b, c \in R$.
- **Lei Comutativa:** $a \cdot b = b \cdot a$ para todo $a, b \in R$.

Propriedade que relaciona $+$ e $\cdot$:

- **Lei Distributiva:** $a \cdot (b + c) = a \cdot b + a \cdot c$ para todo $a, b, c \in R$.

Um anel (comutativo) no qual todo elemento não nulo possui um inverso multiplicativo é chamado de carpo

Divisibilidade

- Sejam a e b elementos de um anel R, com $b \neq 0$. Dizemos que b divide a, ou que a é divisível por b, se existe um elemento $c \in R$ tal que $a = b \cdot c$.
- Seja R um anel. Um elemento $u \in R$ é chamado de unidade se ele possui um inverso multiplicativo, ou seja, se existe um elemento $v \in R$ tal que $u \cdot v = 1$.

Aritmética modular

- 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 $a - b$ for divisível por m. Escrevemos $a \equiv b \pmod{m}$ para indicar que a e b são congruentes módulo m.
- Seja R um anel e seja $m \in R$ com $m \neq 0$. Se $a_1 \equiv a_2 \pmod{m}$ e $b_1 \equiv b_2 \pmod{m}$, então

$$a_1 \pm b_1 \equiv a_2 \pm b_2 \pmod{m}$$
$$a_1 \cdot b_1 \equiv a_2 \cdot b_2 \pmod{m}$$

Anéis Polinomiais e o Algoritmo Euclidiano

- Seja R é um anel qualquer, então podemos criar um anel polinomial com coeficientes retirados de R. Esse anel é denotado por

- $\mathrm{R[x]} = \mathrm{a}_0 + a_1x + a_2x^2 + \ldots + a_nx^n : n \geq 0$ e $a_0, a_1, \ldots, a_n \in R$

  - O grau de um polinômio não nulo é o expoente do maior termo em x que aparece.
  - com $a_n \neq 0$, então $R[x]$ tem grau n.

Divisor Comum

- Um divisor comum de dois elementos $a, b \in F[x]$ é um elemento $d \in F[x]$ que divide tanto a quanto b. Dizemos que d é um maior divisor comum de a e b se todo divisor comum de a e b também divide d.
- Escrevemos $\gcd(a, b)$ para o polinômio mônico único que é um maior divisor comum de a e b.
- O maior divisor comum de $x^2 - 1$ e $x^3 + 1$ é $x + 1$.

Algoritmo Euclidiano estendido para $F[x]$

Seja F um corpo e sejam a e b polinômios em $F[x]$ com $b \neq 0$. Então, o maior divisor comum d de a e b existe, e existem polinômios u e v em $F[x]$ tais que $au + bv = d.a$

Anel Quociente

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

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

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

$$\overline{(\alpha_1 + \beta_1 x) \cdot (\alpha_2 + \beta_2 x)} = \overline{\alpha_1\alpha_2 + (\alpha_1\beta_2 + \alpha_2\beta_1)x + \beta_1\beta_2 x^2} =$$

$$(\alpha_1\alpha_2 - \beta_1\beta_2) + (\alpha_1\beta_2 + \alpha_2\beta_1)x.$$

O algoritmo Euclidiano estendido para polinômios

Dado $a = b \cdot k_1 + r_2$ com $0 \leq \deg r_2 < \deg b$,
$b = r_2 \cdot k_2 + r_3$ com $0 \leq \deg r_3 < \deg r_2$,
$r_2 = r_3 \cdot k_3 + r_4$ com $0 \leq \deg r_4 < \deg r_3$,
$r_3 = r_4 \cdot k_4 + r_5$ com $0 \leq \deg r_5 < \deg r_4$, ...
$r_{t-2} = r_{t-1} \cdot k_{t-2} + r_t$ com $0 \leq \deg r_t < \deg r_{t-1}$, $r_{t-1} = r_t \cdot k_t$.
Então, $d = r_t = \gcd(a, b)$.
Usamos o algoritmo Euclidiano no anel $F_{13}[x]$ para calcular o $\gcd(x^5 - 1, x^3 + 2x - 3)$:
$x^5 - 1 = (x^3 + 2x - 3) \cdot (x^2 + 11) + (3x^2 + 4x + 6)$
$x^3 + 2x - 3 = (3x^2 + 4x + 6) \cdot (9x + 1) + (9x + 4)$
$[\gcd = 9x + 4]$ $3x^2 + 4x + 6 = (9x + 4) \cdot (9x + 8) + 0$
Portanto, $9x + 4$ é o maior divisor comum de $x^5 - 1$ e $x^3 + 2x - 3$ em $F_{13}[x]$.
Para obter um polinômio mônico, multiplicamos por $3 \equiv 9^{-1} \pmod{13}$. Isso nos dá:
$\gcd(x^5 - 1, x^3 + 2x - 3) = x - 1$ em $F_{13}[x]$.

Anéis polinomiais de convolução

Nesta seção, descrevemos o tipo especial de anéis quocientes polinomiais que são usados pelo criptossistema de chave pública NTRU.

Definição. Fixe um inteiro positivo N. O anel de polinômios de convolução (de ordem N) é o anel quociente

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

Da mesma forma, o anel de polinômios de convolução (módulo q) é o anel quociente

$$R_q = (\mathbb{Z}/q\mathbb{Z})[x]/(x^N - 1).$$

Operações

A adição de polinômios corresponde à adição usual de vetores:

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

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

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

onde a soma que define c_k é feita para todos os i e j entre 0 e $N - 1$ue 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 móduloo q.

Example

Vamos calcular o produto $a(x) \cdot b(x)$ no anel $R = \mathbb{Z}[x]/(x^5 - 1)$, considerando: $a(x) = 1 - 2x + 4x^3 - x^4$ e $b(x) = 3 + 4x - 2x^2 + 5x^3 + 2x^4$.
Usando a fórmula $c_k = \sum_{i+j \equiv k \pmod N} a_i b_{k-i}$, temos:

$c_0 = a_0 b_0 = 1 \cdot 3 = 3$

$c_1 = a_0 b_1 + a_1 b_0 = 1 \cdot 4 + (-2) \cdot 3 = -2$

$c_2 = a_0 b_2 + a_1 b_1 + a_2 b_0 = 1 \cdot (-2) + (-2) \cdot 4 + 0 \cdot 3 = -10$

$c_3 = a_0 b_3 + a_1 b_2 + a_2 b_1 + a_3 b_0 = 1 \cdot 5 + (-2) \cdot (-2) + 0 \cdot 4 + 4 \cdot 3 = 21$

$c_4 = a_0 b_4 + a_1 b_3 + a_2 b_2 + a_3 b_1 + a_4 b_0 = 1 \cdot 2 + (-2) \cdot 5 + 0 \cdot (-2) + 4 \cdot 4 + (-1) \cdot 3 = 5$

$c_5 = a_1 b_4 + a_2 b_3 + a_3 b_2 + a_4 b_1 = (-2) \cdot 2 + 0 \cdot 5 + 4 \cdot (-2) + (-1) \cdot 4 = -16$

$c_6 = a_2 b_4 + a_3 b_3 + a_4 b_2 = 0 \cdot 2 + 4 \cdot 5 + (-1) \cdot (-2) = 22$

$c_7 = a_3 b_4 + a_4 b_3 = 4 \cdot 2 + (-1) \cdot 5 = 3$

$c_8 = a_4 b_4 = (-1) \cdot 2 = -2$

Portanto, no anel $R = \mathbb{Z}[x]/(x^5 - 1)$, o produto $c(x)$ de $a(x)$ e $b(x)$ é:
$c(x) = 3 - 2x - 10x^2 + 21x^3 + 5x^4 - 16x^5 + 22x^6 + 3x^7 - 2x^8 =$
$3 - 2x - 10x^2 + 21x^3 + 5x^4 - 16 + 22x + 3x^2 - 2x^3 = -13 + 20x - 7x^2 + 19x^3 + 5x^4$
em $R = \mathbb{Z}[x]/(x^5 - 1)$.
Se trabalharmos em vez disso no anel R_{11}, reduzimos os coeficientes módulo 11 para obter $a(x) \cdot b(x) = 9 + 9x + 4x^2 + 8x^3 + 5x^4$ em $R_{11} = (\mathbb{Z}/11\mathbb{Z})[x]/(x^5 - 1)$.

Centro-lift

Definição. Seja $a(x) \in R_q$. O centro-lift de $a(x)$ para R é o único polinômio $a'(x) \in R$ que satisfaz $a'(x) \mod q = a(x)$ cujo coeficientes são escolhidos no intervalo $-\frac{q}{2} < a'_i \leq \frac{q}{2}$. Por exemplo, se $q = 2$, então o centro-lift de $a(x)$ é um polinômio binário.

Centro-lift

Vamos considerar $N = 5$ e $q = 7$, e o polinômio $a(x) = 5 + 3x - 6x^2 + 2x^3 + 4x^4 \in R_7$. Os coeficientes do centro-lift de $a(x)$ são escolhidos do conjunto $-3, -2, \ldots, 2, 3$, então o centro-lift de $a(x)$ é dado por $-2 + 3x + x^2 + 2x^3 - 3x^4 \in R$.
Da mesma forma, o centro-lift de $b(x) = 3 + 5x^2 - 6x^3 + 3x^4$ é $3 - 2x^2 + x^3 + 3x^4$.

NTRUEncrypt

Começamos fixando um inteiro $N \geq 1$ e dois módulos p e q, e deixamos R, R_p e R_q serem os anéis de polinômios de convolução:

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

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

Podemos visualizar um polinômio $R[x] \in R$ como um elemento de R_p ou R_q ao reduzir seus coeficientes modulo p ou q. Na direção oposta, usamos centro-lifts para mover elementos de R_p ou R_q para R.

Polinômios Ternários

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

$\mathrm{T}(\mathrm{d}_1, d_2) = \{a(x) \in R : a(x)$ possui d_1 coeficientes iguais a 1, d_2 coeficientes iguais a -1, e todos os outros coeficientes iguais a 0

Criptossistema de Chave Pública NTRU

A criação de parâmetros públicos:

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

KeyGeneration:

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

Encryption:m, h

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

Decryption:e, f

- Calcule $f \otimes e \equiv pg \otimes r + f \otimes m \pmod{q}$
- Centro-lifte para $a \in R$ e calcule $m \equiv F_p \otimes a \pmod{p}$
- **return** m

Example

Classe NTRU instanciada com parâmetros $N = 41$, $q = 128$.

Parâmetros públicos:

$$N = 41, \quad q = 128$$

Chave Privada da Alice

Example

A chave privada da Alice consiste em dois polinômios escolhidos aleatoriamente:

$$
\begin{aligned}
f(x) &= x^{40} + x^{39} + x^{37} - x^{36} + x^{35} + x^{33} - x^{32} - x^{31} - x^{30} - x^{27} - x^{26} \\
&\quad - x^{25} + x^{24} + x^{22} - x^{21} + x^{18} + x^{17} - x^{16} + x^{15} - x^{14} - x^{12} - x^{10} \\
&\quad + x^{9} - x^{7} + x^{6} - x^{5} + x^{3} + x + 1 \\
g(x) &= -x^{40} - x^{38} + x^{37} + x^{35} + x^{34} - x^{33} + x^{31} + x^{29} + x^{27} - x^{25} + x^{\cdots} \\
&\quad - x^{21} - x^{20} + x^{19} + x^{18} + x^{16} - x^{15} + x^{14} - x^{13} - x^{11} + x^{10} + x^{9} \\
&\quad - x^{8} - x^{7} - x^{6} - x^{5} + x^{3} - x^{2} + x
\end{aligned}
$$

Chave Pública da Alice

Example

Alice calcula os inversos:

$$
\begin{aligned}
Fq(x) &= f(x)^{-1} \mod q \\
&= 81x^{40} + 108x^{39} + 41x^{38} - 91x^{37} + 105x^{36} - 86x^{35} - 23x^{34} \\
&- 32x^{33} + 87x^{32} + 73x^{31} + 30x^{30} - 49x^{29} - 79x^{28} + 10x^{27} + 101x \\
&+ 102x^{25} + 54x^{24} - 57x^{23} + 26x^{22} - 65x^{21} + 90x^{20} + 103x^{19} \\
&+ 75x^{18} - 9x^{17} + 100x^{16} + 90x^{15} - 104x^{14} + 97x^{13} + 78x^{12} \\
&+ 118x^{11} + 102x^{10} - 87x^{9} - 100x^{8} - 22x^{7} - 12x^{6} + 25x^{5} \\
&- 47x^{4} + 51x^{3} + 35x^{2} - 59x - 91
\end{aligned}
$$

Chave Pública da Alice (Continuação)

Example

Alice armazena $f(x)$ e $Fp(x)$ como sua chave privada e calcula e publica sua chave pública:

$$\begin{aligned} h(x) &= Fp(x) \cdot g(x) \\ &= 36x^{40} - 40x^{39} + x^{38} - 18x^{37} - 63x^{36} - 46x^{35} + 10x^{34} + 34x^{33} \\ &+ 10x^{32} + 57x^{31} - 4x^{30} + 50x^{29} + 14x^{28} - 50x^{27} - 25x^{26} + 61x^{25} \\ &+ 28x^{24} + 60 \end{aligned}$$

Cifragem por Bob

Example

Bob calcula e envia para Alice o texto cifrado:

$$
\begin{aligned}
e(x) &= pr(x) \cdot h(x) + m(x) \\
&= 3x^{40} - 63x^{39} + 62x^{38} - 10x^{37} + 58x^{36} - 60x^{35} + 4x^{34} - 38x^{33} \\
&- 41x^{32} + 35x^{24} + 49x^{23} - 14x^{31} + 26x^{30} - 15x^{29} - 5x^{28} + 18x^{27} \\
&- 60x^{26} + x^{25} - 37x^{15} + 23x^{14} - 34x^{22} - 42x^{21} - 58x^{20} + 37x^{19} \\
&- 47x^{18} - 50x^{17} - 16x^{16} + 32x^{13} - 9x^{12} + 6x^{11} - 62x^{10} - 54x^{9} \\
&+ 41x^{8} + 61x^{7} - 59x^{6} - 31x^{5} + 19x^{4} - 27x^{3} - 39x^{2} - 43x + 58
\end{aligned}
$$

Descriptografia por Alice

Example

Para descriptografar a mensagem, Alice realiza as seguintes etapas:

1. Calcula $f \cdot e \equiv p \cdot g \cdot r + f \cdot m \pmod{q}$
2. Centraliza para $a \in \mathbb{R}$
3. Compute $m \equiv Fp \cdot a \pmod{p}$

Agora, Alice obteve a mensagem descriptografada m.

$$m(x) = x^{16} + x^{15} - x^{14} + x + 1$$

Bibliografia

Chen, L. et al. **Report on post-quantum cryptography**. Volume 12. US Department of Commerce, National Institute of Standards and Technology, 2016.

Hoffstein, J.; Pipher, J.; and Silverman, J. H. **NTRU: A ring-based public key cryptosystem.** In: International Algorithmic Number Theory Symposium, Springer, 1998, p. 267-288.

Luciano, D. and Prichett, G. **Cryptology: From Caesar ciphers to public-key cryptosystems**. *The College Mathematics Journal*, Taylor & Francis, 1987.

Shor, P. W. **Algorithms for quantum computation: Discrete logarithms and factoring**. In: Proceedings of the 35th Annual Symposium on Foundations of Computer Science, IEEE, 1994, p. 124-134.

Obrigado pela atenção!