Análise Álgebrica de um Esquema Criptográfico Multivariado Utilizando Bases de Gröbner

Guilherme Cappelli
Orientador: Cláudio Miceli

Semana de Integração Acadêmica da UFRJ

23/09/2025

Sumário

Conteúdo

Criptografias de Chave Pública Multivariada

- Multivariate Public Key Cryptosystems - MPKC - é uma família de criptografias baseadas em funções em várias variáveis sob um corpo finito como chave pública.
- É evidente que, por usar chave pública, estas serão Criptografias Assimétricas, diferentemente de Cifras de Feistel ou o próprio AES.

Corpo Finito

Um corpo finito $\mathbb{F}$ é um corpo cuja ordem $q \in \mathbb{N}$ é finita, para q um número primo.

- Ex: $\mathbb{F}_2$ (Corpo binário)
- Ex: Os inteiros módulo 11 $(\mathbb{Z}/11\mathbb{Z})$

Problemas NP-Difícil

- Sistemas de criptografia devem se basear em problemas difíceis de serem solucionados computacionalmente para a *trapdoor*.
- Nas Criptografias de Curvas Elípticas, como a Variante de Menezes e Vanstone para o ElGamal, é adotado o Problema do Logaritmo Discreto.
- Para o RSA, a maior dificuldade é fatorar $n = p \cdot q$, pois uma vez feito isso, calcular $\phi(n) = (p-1) \cdot (q-1)$ é trivial, e portanto, $e \cdot d \equiv 1 \mod \phi$.
- A segurança dos esquemas MPKC é baseada na dificuldade de encontrar soluções para um sistema de equações de polinômios em várias variáveis, conhecido como o *Multivariate Polynomial Problem*.
- Se esse sistema for composto apenas por polinômios quadráticos se chama *Multivariate Quadratic Problem*, ou ainda, **Problema MQ**.

Base de Gröbner

Definição

Um subconjunto $G \subset I$ é uma base de Gröbner para I se in(I) for gerado pelos in(g), para cada $g \in G$. (Adaptado de S. C. Coutinho, **Polinômios e Computação Algébrica**)

Propriedades Importantes

- Seja G é uma base de Gröbner de I. Então G gera I.
- Sob a ordem monomial $>_{lex}$, possui formato triangular (reduzida).
- Formato Triangular implica resolução simplificada.

Conteúdo

Modificadores de Segurança

Modificador 'Menos'

- Polinômios são removidos do mapeamento central F, restando os primeiros $(n+1-a)$ polinômios.
- a próximo de $\lfloor \log_2(n) \rfloor$

Modificador 'Mais'

- Acrescenta s polinômios quadráticos aleatórios à chave pública, onde foi implementado o método anterior.
- Torna o mapeamento central F em injetivo.
- Assim, $P : \mathbb{F}^n \to \mathbb{F}^m$, onde $m = n + 1 - a + s$.

- Decriptar mensagem se torna muito mais custoso, apesar de adicionar uma camada de segurança extra contra ataques de Linearização.

Conteúdo

Criptografia de Chen et al.

- Primeiramente, vamos construir a ideia do mapeamento central da chave pública $P = S \circ F \circ T$.
- Seja $\mathbb{F}[x_1, \ldots, x_n]$ um anel de polinômios sobre um corpo finito de ordem q. Suponha que a característica de $\mathbb{F}$ não seja 2.
- Sejam $C \in \mathbb{F}^{(n+1)\times n}$ uma matriz e os polinômios $f_1, .., f_{n+1} \in \mathbb{F}[x_1, \ldots, x_n]$. Estruturamos esse sistema como o problema MQ enunciado anterioremente.

Sistema Base

$$\begin{cases} f_1 = (x_1 - c_{1,1})^2 + \cdots + (x_n - c_{1,n})^2, \\ \quad \vdots \\ f_{n+1} = (x_1 - c_{n+1,1})^2 + \cdots + (x_n - c_{n+1,n})^2 \end{cases}$$

Criptografia de Chen et al.

- Queremos solucionar esse sistema para $y = (y_1, \ldots, y_{n+1}) \in \mathbb{F}^{(n+1)}$, então se tomarmos a diferença entre equações de f_{i+1} e f_i, para todo $1 \leq i \leq n$, obtemos

$$\begin{cases} f_2 - f_1 = y_2 - y_1 \\ \quad \vdots \\ f_{n+1} - f_n = y_{n+1} - y_n \end{cases}$$

- Como $f_i = (x_1^2 - 2 \cdot x_1 \cdot c_{i,1} + c_{i,1}^2) + \cdots + (x_n^2 - 2 \cdot x_n \cdot c_{i,n} + c_{i,n}^2)$, podemos agrupar esses termos pelo grau.

$$f_i = (\sum_{j=0}^{n} x_j^2) - 2 \cdot (\sum_{k=0}^{n} x_k \cdot c_{i,k}) + (\sum_{l=0}^{n} c_{i,l}^2)$$

- O que nos leva a

$$f_{i+1} - f_i = 2 \cdot (\sum_{k=0}^{n} x_k \cdot (c_{i,k} - c_{i+1,k})) + (\sum_{l=0}^{n} c_{i+1,l}^2 - c_{i,l}^2)$$

Criptografia de Chen et al.

- Sabemos do sistema inicial que $f_{i+1} - f_i = y_{i+1} - y_i$. Então, se definirmos a matriz $C' := (2 \cdot (c_{i,j} - c_{i+1,j}))_{i,j} \in \mathbb{F}^{n \times n}$, obtemos o seguinte sistema.

$$\begin{bmatrix} y_2 - y_1 \\ y_3 - y_2 \\ \vdots \\ y_{n+1} - y_n \end{bmatrix} = C' \cdot \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} + \begin{bmatrix} \sum_{k=1}^{n} (c_{2,k}^2 - c_{1,k}^2) \\ \sum_{k=1}^{n} (c_{3,k}^2 - c_{2,k}^2) \\ \vdots \\ \sum_{k=1}^{n} (c_{n+1,k}^2 - c_{n,k}^2) \end{bmatrix}$$

- Se construirmos C para que C' tenha inversa, o sistema possui solução única, o que vai ser bastante desejável para a criptografia.

Criptografia de Chen et al.

- Para a implementação dos modificadores da seção 3 escolha os primeiros $(n+1-a)$ polinômios de $f_1, \ldots, f_{n+1}$, chamaremo-os F'_α
- Escolha $g_1, \ldots, g_s \in \mathbb{F}[x_1, \ldots, x_n]$ polinômios de grau 2 de forma aleatória, denote o conjunto desses como G
- Faça a união $F'_\alpha \cup G$ no mapeamento central F, onde $a, s \in \mathbb{Z}^+$ e como é fácil perceber $m = n + 1 - a + s$.

$$F = (f_1, f_2, \ldots, f_{n+1-a}, g_1, \ldots, g_s) \in \mathbb{F}^m[x_1, \ldots, x_n] \tag{1}$$

- Considere dois mapeamentos afins invertíveis $S : \mathbb{F}^n \to \mathbb{F}^n, T : \mathbb{F}^m \to \mathbb{F}^m$ e denote a *chave pública* do criptosistema como $P : \mathbb{F}^n \to \mathbb{F}^m$ e calcule-a com $P = S \circ F \circ T$. Enquanto isso, a *chave privada* será a quádrupla (C, G, T, S).

Criptografia de Chen et al.

Algoritmo 1 - Computando Chave Pública P

func pubkey(S, F, T, x):

$\mathbf{v} \leftarrow S \cdot x + s$

$\mathbf{v}_1 \leftarrow F(\mathbf{v})$

$\mathbf{P} \leftarrow T \cdot \mathbf{v}_1 + \mathbf{t}$

return P

Encriptando uma mensagem

- Seja pt uma mensagem a ser encriptada, após sua codificação ela se torna $\alpha \in \mathbb{F}^n$.
- O processo de encriptar é feito facilmente através de $y = P(\alpha) \in \mathbb{F}^m$. Já decriptar um *ciphertext* é um pouco mais trabalhoso, visto que exige realizarmos as operações inversas recursivamente de $\alpha = T^{-1} \circ F^{-1} \circ S^{-1}$.

Conteúdo

Obtendo plaintext via Bases de Gröbner

Definição 1

Seja $P \in \mathbb{F}^m$ um vetor com polinômios de grau 2 sobre as variáveis $x_1, \ldots, x_n$, a função $\text{Quad} : \mathbb{F}^m[x_1, \ldots, x_n] \to \mathbb{F}^{m \times n}$ armazena os coeficientes dos termos quadráticos dos polinômios em uma matriz de dimensão $m \times n$.

- Para ilustrar o comportamento desta função, segue o exemplo.
- Sejam $P = [5x_1^2, \quad x_1^5, \quad x_1^2] \in \mathbb{F}^3[x_1]$.

$$\text{Quad}(P) = \begin{bmatrix} 5 \\ 0 \\ 1 \end{bmatrix}$$

Obtendo plaintext via Bases de Gröbner

Enunciado

O espaço **span**(P) é gerado por $(n-a)$ polinômios lineares e $(s+1)$ polinômios quadráticos, pela construção do mapeamento central.

- Seja $M := [\text{Quad}(p_1), \text{Quad}(p_2), \ldots, \text{Quad}(p_m)] \in \mathbb{F}^{m \times n}$, para $p_i \in P$.
- Por construção de F, existem apenas $(n-a)$ polinômios de grau 1 na função regular, logo o subespaço da solução de todos $\sum_{i=1}^{m} z_i \cdot \text{Quad}(p_i) = 0$ também terá dimensão $(n-a)$.

Obtendo plaintext via Bases de Gröbner

- Nesse sentido, sejam os vetores linearmente independentes que formam uma base para o espaço de soluções para o núcleo da matriz M, $Z = \{z_1^{(i)}, \ldots, z_m^{(i)}\} \in \mathbb{F}^m$, para $1 \leq i \leq (n-a)$, assim temos o sistema

$$\begin{cases} k_1(x_1, \ldots, x_n) = z_1^{(1)} \cdot p_1 + \cdots + z_m^{(1)} \cdot p_m \\ \vdots \\ k_{n-a}(x_1, \ldots, x_n) = z_1^{(n-a)} \cdot p_1 + \cdots + z_m^{(n-a)} \cdot p_m \end{cases}$$

- Sendo assim, **span**(P) é gerado por $k_1, \ldots, k_{n-a}$ e outros $(s+1)$ polinômios quadráticos.
- Lembre que esses polinômios lineares vieram diretamente da chave pública.

Obtendo plaintext via Bases de Gröbner

- Queremos então que os polinômios da chave pública sejam iguais ao *ciphertext* $y \in \mathbb{F}^m$. Isso acontece se $p_i - y_i = 0$, para todo $1 \leq 1 \leq m$.
- Com as informações do slide anterior, podemos reduzir o problema MQ, propondo que se $y = P$, (substituindo) $\sum_{i=1}^{m} z_i^{(j)} \cdot p_i = \sum_{i=1}^{m} z_i^{(j)} \cdot y_i$, para $1 \leq j \leq (n-a)$.

Obtendo plaintext via Bases de Gröbner

- Como passo final do algoritmo, rodamos Gröbner no sistema abaixo, que nos dará α tal que $P(\alpha) = y$.

Ataque de Gröbner

$$\begin{cases} p_1 - y_1 = 0 \\ p_2 - y_2 = 0 \\ \vdots \\ p_m - y_m = 0 \\ \sum_{i=1}^{m} z_i^{(1)} \cdot p_i - \sum_{i=1}^{m} z_i^{(1)} \cdot y_i = 0 \\ \vdots \\ \sum_{i=1}^{m} z_i^{(n-a)} \cdot p_i - \sum_{i=1}^{m} z_i^{(n-a)} \cdot y_i = 0 \end{cases}$$

Obtendo plaintext via Bases de Gröbner

- O resultado de computarmos a base de Gröbner reduzida do ideal J, nos dá um ideal de formato triangular.
- Obtemos polinômios na forma $x_i - \alpha_i$, para $1 \leq i \leq n$, onde α_i é um elemento do vetor da mensagem codificada.

$$J = \langle p_1 - y_1, \ldots, p_m - y_m, \sum_{i=1}^{m} z_i^{(1)} \cdot p_i - \sum_{i=1}^{m} z_i^{(1)} \cdot y_i, \ldots, \sum_{i=1}^{m} z_i^{(n-a)} \cdot p_i - \sum_{i=1}^{m} z_i^{(n-a)} \cdot y_i \rangle$$

- Sendo assim, basta efetuarmos $(x_i - (x_i - \alpha_i)) = \alpha_i$ em $\mathbb{F}$ e decodificarmos a mensagem.

Referências

- IKEMATSU, Yasuhiko; NAKAMURA, Shuhei. *Security Analysis via Algebraic Attack Against "A New Encryption Scheme for Multivariate Quadratic System"*.
- CHEN, Jiahui; NING, Jianting; LING, Jie; LAU, Terry Shue Chien; WANG, Yacheng. *A new encryption scheme for multivariate quadratic systems*.
- SOBRAL, João Victor Pacheco. *On the Security of Multivariate Encryption Schemes*.
- PERRET, Ludovic. *Gröbner Bases Techniques in Post-Quantum Cryptography*.
- PATARIN, Jacques. *Cryptanalysis of the Matsumoto and Imai Public Key Scheme of Eurocrypt'88*.
- PATARIN, Jacques; GOUBIN, Louis; COURTOIS, Nicolas. C^*_{-+} and HM: Variations Around Two Schemes of T. Matsumoto and H. Imai.

Até a próxima

Obrigado!

Figure: Link para os slides no meu site.

Mapeamento Afim

Definição

Um mapeamento afim $S := (S_{matriz}, s_{vetor}) : \mathbb{F}^m \to \mathbb{F}^m$ é definido como:

$$\begin{bmatrix} y_1 \\ \vdots \\ y_m \end{bmatrix} = S_{matriz} \cdot \begin{bmatrix} x_1 \\ \vdots \\ x_m \end{bmatrix} + s_{vetor}$$

Propriedades Importantes

- Preserva estrutura linear
- Facilmente invertível quando S_{matriz} é inversível
- Usado para mascarar a estrutura do sistema central

Multivariate Quadratic Problem

Problema MQ

Sejam $\mathbb{F}[x_1, \ldots, x_n]$ um anel de polinômios sobre um corpo finito $\mathbb{F}$ e os polinômios quadráticos $f_1, \ldots, f_m \in \mathbb{F}[x_1, \ldots, x_n]$, para $m > n$. O sistema de equações dos polinômios $f_1, \ldots, f_m$ que constrói o problema MQ é:

$$\begin{cases} f_1(x_1, \ldots, x_n) = \sum_{1 \le i \le j \le n} {a_{ij}}^{(1)} \cdot x_i \cdot x_j + \sum_{1 \le i \le n} {b_i}^{(1)} \cdot x_i + c^{(1)} = d_1 \\ \qquad \vdots \\ f_m(x_1, \ldots, x_n) = \sum_{1 \le i \le j \le n} {a_{ij}}^{(m)} \cdot x_i \cdot x_j + \sum_{1 \le i \le n} {b_i}^{(m)} \cdot x_i + c^{(m)} = d_m \end{cases}$$

onde todos $a_{ij}, b_{ij}, c \in \mathbb{F}$.

- Problema NP-difícil sobre corpos finitos, até mesmo para $\mathbb{F}_2$.

Decriptando uma mensagem

- Seja $P(\alpha) = y \in \mathbb{F}^m$ o *ciphertext* a ser decriptado. Por construção, os dois mapeamentos afins S e T são invertíveis, logo $\beta = (\beta_1, \ldots, \beta_m) := T^{-1} \circ y$. Denote $\beta' \in \mathbb{F}^a[x_1, \ldots, x_n]$ para o laço atual.

$$\begin{cases} f_1(x_1, \ldots, x_n) = \beta_1 \\ \vdots \\ f_{n+1-a}(x_1, \ldots, x_n) = \beta_{n+1-a} \\ f_{n+1-a+1}(x_1, \ldots, x_n) = \beta'_1 \\ \vdots \\ f_{n+1}(x_1, \ldots, x_n) = \beta'_a \end{cases}$$

- Relembre a construção do sistema para que C' fosse invertível, é aqui que ela se torna fundamental.

$$\gamma = C'^{-1} \cdot \left(\begin{bmatrix} \beta_2 - \beta_1 \\ \vdots \\ \beta'_a - \beta'_{a-1} \end{bmatrix} - \begin{bmatrix} \sum_{k=1}^{n} (c_{2,k}^2 - c_{1,k}^2) \\ \sum_{k=1}^{n} (c_{3,k}^2 - c_{2,k}^2) \\ \vdots \\ \sum_{k=1}^{n} (c_{n+1,k}^2 - c_{n,k}^2) \end{bmatrix} \right)$$

Decriptando uma mensagem

- Por conta do Modificador 'Mais', precisamos verificar se para cada $g_i \in G$, vale a igualdade

$$\begin{cases} g_1(\gamma) = \beta_{n+1-a+1} \\ \vdots \\ g_s(\gamma) = \beta_m \end{cases}$$

- Se não o for, escolha outro $\beta' \in \mathbb{F}^a[x_1, \dots, x_n]$ e repita o processo
- Caso contrário, damos prosseguimento à decriptação e calculamos $\alpha = S^{-1} \circ \gamma$, que é a resposta que procuramos para $P(\alpha) = y$.

Obtendo plaintext via Bases de Gröbner

- Esse ataque foi proposto por **Ikematusu** e **Nakamura**.
- Dados uma chave pública $P \in \mathbb{F}^m[x_1, \ldots, x_n]$ e o ciphertext $y = (y_1, \ldots, y_m) \in \mathbb{F}^m$ para a criptografia de Chen et al.
- Considere $h_i = f_{i+1} - f_i$, que por construção tem grau$(h_i) = 1$, para todo $1 \leq i \leq n - a$.
- Como construímos C para que C' seja invertível, o conjunto $\{h_1, \ldots, h_{n-a}\}$ é linearmente independente e, portanto,

$$\textbf{span}(F) = \{h_1, \ldots, h_{n-a}, f_1, g_1, \ldots, g_s\}$$

.

Relembrando...

Proposição 1

Se uma matriz quadrada $C' \in \mathbb{F}^{n \times n}$ é invertível, então suas colunas são linearmente independentes.

Demonstração: Como C' é invertível, então existe uma matriz quadrada $B \in \mathbb{F}^{n \times n}$ tal que $C' \times B = B \times C' = I$. Suponha, por absurdo, que as colunas de C' são linearmente dependentes. Então, por haver uma redundância nesses vetores, deve existir $\vec{v} \neq \overline{0}$ tal que $C' \cdot \vec{v} = \overline{0}$. Contudo, isso implica em $B \cdot C' \cdot \vec{v} = \overline{0} \Longrightarrow I \cdot \vec{v} = \overline{0} \Longrightarrow \vec{v} = \overline{0}$, que é uma contradição. Portanto, C' é linearmente independente. $\square$

Obtendo plaintext via Bases de Gröbner

Proposição 2

Sejam $S : \mathbb{F}^n \to \mathbb{F}^n$ e $T : \mathbb{F}^m \to \mathbb{F}^m$ mapeamentos afins invertíveis e $F = (f_1, \ldots, f_m) \in \mathbb{F}^m$ uma função regular. Se $P = S \circ F \circ T$,então

$$\textbf{span}(P) = \textbf{span}(F) \circ T$$

Demonstração: Seja V o domínio inicial dos vetores. Denotamos o $\textbf{span}(P)$ como $\textbf{span}_P(V) = \text{Span}\{P(v) \mid v \in V\}$, então substituindo $P = S \circ F \circ T$ no span,

$$\textbf{span}_P(V) = \text{Span}\{S(F(T(v))) \mid v \in V\}$$

Contudo, S é invertível e a linearidade implica $S(\text{Span}\{F(T(v)) \mid v \in V\})$.

$$\textbf{span}_P(V) = S(\text{Span}_{F \circ T}(V))$$

Portanto,

$$\textbf{span}(P) = \textbf{span}(F) \circ T \qquad \square$$

Obtendo plaintext via Bases de Gröbner

- Segue pela **Proposição 2**, que **span**$(P) =$ **span**$(F) \circ T$, que é

$$\textbf{span}(P) = \{h_1 \circ T, \ldots, h_{n-a} \circ T, f_1 \circ T, g_1 \circ T, \ldots, g_s \circ T\}$$

- Podemos concluir que **span**(P) é L.I., porque T também é linearmente independente.
- Além disso, a partir de uma chave pública P, podemos gerar um conjunto linearmente independente de $(n-a)$ polinômios lineares, já que **span**(P) consiste de $(n-a)$ polinômios de grau 1 e $(s+1)$ polinômios quadráticos.