Proceeding Series of the Brazilian Society of Computational and Applied Mathematics, v. 12, n. 1, 2026.

Trabalho apresentado no XLIV CNMAC, Fundação Getulio Vargas - Rio de Janeiro - RJ, 2025.

Proceeding Series of the Brazilian Society of Computational and Applied Mathematics

Comparação de Algoritmos de Interpolação em Secret Sharing

Thays Rocha[1], Renato Borseti[2], Fábio Borges[3]
Laboratório Nacional de Computação Científica (LNCC), Petrópolis, RJ

Resumo. Este artigo tem como objetivo explorar e comparar diferentes algoritmos de interpolação que podem substituir o método de Lagrange no contexto do esquema criptográfico Shamir Secret Sharing. Serão analisados métodos alternativos de interpolação, comparando seu desempenho computacional. Além disso, será avaliado o tempo de execução em função do número de *shares*, variável que influencia diretamente a eficiência do sistema, especialmente em aplicações reais, como autenticação multifator e preservação da privacidade em dados de redes elétricas.

Palavras-chave. Interpolação, Shamir Secret Sharing, Criptografia, Lagrange, Newton e Vandermonde

1 Introdução

A segurança da informação é um dos pilares fundamentais na sociedade digital contemporânea, especialmente em cenários que exigem o armazenamento e a proteção de dados sensíveis. Conforme [3], é de suma importância a prevenção de ataques tanto de terceiros quanto internos.

Com isso, métodos criptográficos estão cada vez mais presentes. Com o *Shamir Secret Sharing* é possível garantir a privacidade e a integridade desses dados, pois, além de armazená-los, também podemos realizar cálculos matemáticos em seus valores cifrados, como demonstrado em [4].

Assim, neste artigo, o objetivo é explorar e comparar diferentes algoritmos de interpolação que podem substituir o método de Lagrange no contexto do *Shamir Secret Sharing*. Serão analisados e comparados os métodos de Newton e Vandermonde, como métodos alternativos de interpolação, em busca de melhor desempenho computacional.

Além disso, será analisado o tempo de execução em função do número de *shares*, uma variável de suma importância, tendo em vista que impacta diretamente na eficiência do sistema como um todo. Isso se deve ao fato de que o aumento exponencial da quantidade de *shares* tem implicações diretas na performance do sistema, sendo crucial entender essas variáveis para aplicações práticas, principalmente em sistemas distribuídos.

O conteúdo das próximas seções está organizado da seguinte forma: A Seção 2 apresenta o método de Computação Segura de Múltiplas Partes, conhecido como *Shamir Secret Sharing*. Em seguida, na Seção 3, é fornecido um resumo dos métodos de interpolação a serem considerados para o presente trabalho, a saber: Newton e Vandermonde. Na Seção 4, abordamos o experimento feito, com as configurações utilizadas, alterações realizadas, tanto do método de interpolação, quanto no número de *shares* utilizados, e a análise feita referente aos resultados obtidos. Por fim, na Seção 5, são apresentadas as considerações finais e os interesses referentes a trabalhos futuros.

[1]academicthaysrocha@gmail.com
[2]renato.borseti@gmail.com
[3]borges@lncc.br

2 Shamir Secret Sharing

O *Shamir Secret Sharing*, ou Compartilhamento de Segredo de Shamir em português, pertence ao campo de *Multi-Party Computation* (MPC) em criptografia, que tem como finalidade desenvolver abordagens em que seu processamento é compartilhado entre várias partes, sem que elas possuam o conhecimento sobre as outras partes. O *Shamir Secret Sharing*, proposto por [5], para realizar tal feito, baseia-se na interpolação de Lagrange no Corpo Finito, descrito abaixo por [2].

Teorema 2.1. *Seja $f : \mathbb{R} \to \mathbb{R}$ uma função conhecida em $n+1$ pontos distintos $x_0, x_1, \ldots, x_n$, com os respectivos valores $f(x_0), f(x_1), \ldots, f(x_n)$. O* ***polinômio interpolador de Lagrange*** *é definido como:*

$$P_n(x) = \sum_{i=0}^{n} f(x_i)\ell_i(x), \tag{1}$$

onde os ***polinômios básicos de Lagrange*** *$\ell_i(x)$ são dados por:*

$$l_i(x) = \prod_{\substack{j=0 \\ j\neq i}}^{n} \frac{x - x_j}{x_i - x_j}. \tag{2}$$

A construção do polinômio interpolador de Lagrange garante que $P_n(x)$ satisfaz a condição de interpolação, ou seja, $P_n(x_i) = f(x_i)$ para todo $i = 0, 1, \ldots, n$. Além disso, a interpolação polinomial de Lagrange é única, sendo o único polinômio de grau no máximo n que interpola os dados fornecidos.

Seu passo a passo é descrito a seguir:

Etapa 1. Dealer $\mathcal{D}$ escolhe o grande primo p, que o corpo será definido, e com o segredo s gera o polinômio de grau $k-1$ da forma:

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{k-1}x^{k-1} \bmod p, \tag{3}$$

onde $a_0 = s$, $p > n$ e $a_0, a_1, \cdots a_{k-1} \in \mathbb{Z}_p$ são escolhidos aleatoriamente, exceto a_0.

Etapa 2. $\mathcal{D}$ calcula as n partes do processo:

$$\text{share}_i = (i, f(i)), \tag{4}$$

e envia para cada um dos $\mathcal{P}_i$ via canal seguro, com $i = 1$ a n.

Etapa 3. Para a reconstrução assumimos que[4] $\{\mathcal{P}_i\}_{i=1}^{k}$ enviem suas *shares* $\{s_i\}_{i=1}^{k}$. Usando a interpolação de Lagrange com suas *shares*, encontramos o segredo da seguinte forma:

$$s = a_0 = f(0) = \sum_{i=1}^{k} f(i) \prod_{j=1, j\neq i}^{k} \frac{-j}{(i-j)} \mod p. \tag{5}$$

[4]Neste caso, estamos sinalizando a variação na cardinalidade, não o índice de participantes.

DOI: 10.5540/03.2026.012.01.0264

3 Métodos de Interpolação

Nesta seção, abordamos os métodos de interpolação considerados para utilizar na reconstrução dos dados no contexto do *Secret Sharing*. A interpolação é uma técnica essencial para estimar valores desconhecidos a partir de um conjunto de dados discretos, e, neste estudo, exploramos dois métodos amplamente utilizados: o método de Newton e o método de Vandermonde. Cada subseção a seguir apresenta um resumo dos métodos, com o objetivo de fornecer uma compreensão de como essas abordagens podem ser aplicadas e os impactos que geram nos resultados da reconstrução de dados.

3.1 Newton

O método de interpolação de Newton é um método numérico utilizado para encontrar um polinômio, baseado em diferenças divididas para calcular coeficientes. Esse método é eficiente para adicionar novos pontos sem recalcular toda a interpolação. Tal método é muito útil quando temos fatores de autenticação extra como, por exemplo, um sistema Multi Factor Authentication - Autenticação MultiFator (MFA), como em [1]. O método aqui apresentado está de acordo com [2],

Teorema 3.1. *Seja $f : \mathbb{R} \to \mathbb{R}$ uma função conhecida em $n+1$ pontos distintos $x_0, x_1, \ldots, x_n$, com os respectivos valores $f(x_0), f(x_1), \ldots, f(x_n)$. O polinômio interpolador de Newton é definido como:*

$$\begin{aligned} P_n(x) = f[x_0] + f[x_0, x_1](x - x_0) + f[x_0, x_1, x_2](x - x_0)(x - x_1) \\ + \ldots + f[x_0, x_1, \ldots, x_n](x - x_0)(x - x_1)\ldots(x - x_{n-1}), \end{aligned} \tag{6}$$

onde os coeficientes $f[x_0, x_1, \ldots, x_k]$ são as diferenças divididas de f, definidas recursivamente por:

$$f[x_i] = f(x_i), \tag{7}$$

$$f[x_i, x_{i+1}, \ldots, x_{i+k}] = \frac{f[x_{i+1}, \ldots, x_{i+k}] - f[x_i, \ldots, x_{i+k-1}]}{x_{i+k} - x_i}, \quad k \geq 1. \tag{8}$$

3.2 Vandermonde

A interpolação de Vandermonde utiliza um sistema linear baseado em uma matriz com potências dos valores de entrada para determinar os coeficientes de um polinômio interpolador. Dado um conjunto de $n+1$ pontos $(x_0, y_0), (x_1, y_1), \ldots, (x_n, y_n)$, onde todos os x_i são distintos, o objetivo é encontrar os coeficientes $a_0, a_1, \ldots, a_n$ de um polinômio $P(x)$ na forma, conforme [2]:

$$P(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n, \tag{9}$$

tal que, $P(x_i) = y_i$ para cada $i = 0, 1, \ldots, n$.

Ao substituir cada par (x_i, y_i) na equação do polinômio, obtemos um sistema de equações lineares:

$$\begin{aligned} a_0 + a_1 x_0 + a_2 x_0^2 + \cdots + a_n x_0^n &= y_0, \\ a_0 + a_1 x_1 + a_2 x_1^2 + \cdots + a_n x_1^n &= y_1, \\ &\vdots \\ a_0 + a_1 x_n + a_2 x_n^2 + \cdots + a_n x_n^n &= y_n. \end{aligned} \tag{10}$$

DOI: 10.5540/03.2026.012.01.0264

Este sistema pode ser escrito na forma matricial como $VA = Y$, onde A é o vetor dos coeficientes ($[a_0, a_1, \ldots, a_n]^T$), Y é o vetor dos valores y ($[y_0, y_1, \ldots, y_n]^T$), e V é a matriz de Vandermonde:

$$V = \begin{pmatrix} 1 & x_0 & x_0^2 & \ldots & x_0^n \\ 1 & x_1 & x_1^2 & \ldots & x_1^n \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & x_n^2 & \ldots & x_n^n \end{pmatrix}. \tag{11}$$

O determinante da matriz de Vandermonde é dado por:

$$\det(V) = \prod_{0 \leq i < j \leq n} (x_j - x_i). \tag{12}$$

4 Experimento

Nesta seção, apresentamos os detalhes experimentais realizados para a análise dos impactos das mudanças nos parâmetros e nos métodos utilizados em nossa simulação. A primeira subseção descreve a configuração da máquina utilizada. Em seguida, discutimos a análise da alteração do método de interpolação, investigando como diferentes técnicas afetam o desempenho e os resultados da simulação. Posteriormente, abordamos a análise da alteração do número de *shares* necessários para a reconstrução do *Secret Sharing*, explorando o impacto dessa modificação no sistema. Por fim, analisamos todos os dados resultantes obtidos.

4.1 Configurações

Para a simulação dos cenários apresentados, o código foi criado na linguagem *Python* versão 3.11.9, executado por meio do *Integrated Development Environment* (IDE) Visual Studio Code versão 1.95, em um computador Intel Core I3 com 4 GB de memória e um *Solid-State Drive* (SSD) de 480 GB. Para verificação do tempo de desempenho de cada algoritmo foi utilizado a função ***perf_ counter()***, que retorna o tempo em segundos, como número de ponto flutuante.

4.2 Alteração do Método de Interpolação

Diferentes técnicas de interpolação podem ter impactos significativos nos resultados, e esta análise busca comparar como essas variações influenciam a reconstrução dos dados no contexto de *Secret Sharing*. Para garantir uma avaliação precisa e isolar a influência da técnica de interpolação, todos os demais parâmetros do experimento foram mantidos constantes, como exposto na Tabela 1 abaixo.

Tabela 1: Parâmetros básicos.

Cenário 1	
Corpo Finito	36313
Número de *shares*	5
Threshold (k)	3
Segredo	23

Reestruturamos o *Shamir Secret Sharing* substituindo a interpolação tradicional de Lagrange pelos métodos de Newton e de Vandermonde, com o objetivo de analisar o desempenho computacional desta alteração. E com isso temos os tempos de execução obtidos para cada uma das

técnicas analisadas, que são apresentados na Tabela 2, permitindo uma comparação quantitativa dos efeitos das diferentes escolhas de interpolação.

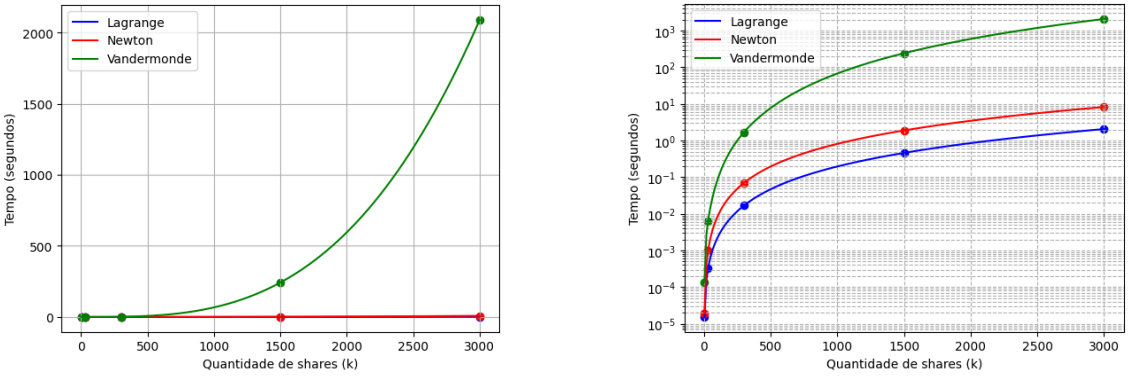
Tabela 2: Parâmetros básicos.

	Lagrange	Newton	Vandermonde
Valor recuperado	23	23	23
Tempo de processamento	$8.8661 \cdot 10^{-06}$	$1.2499 \cdot 10^{-05}$	5.0692

4.3 Alteração do Número de *shares*

Esta subseção examina o impacto da modificação do número de *shares* necessários para a reconstrução do *Secret Sharing*.

Temos na Figura 1 o gráfico resultante do tempo médio, em segundos, para o mesmo conjunto de *shares* (k) necessários para a reconstrução do segredo, para cada algoritmo de interpolação. A análise considerou valores de $3, 30, 300, 1500$ e 3000 para k (*threshold*), de modo a evidenciar melhor a curva de crescimento. O tempo registrado para cada método corresponde à média obtida em 100 simulações, garantindo resultados mais consistentes e reduzindo variações indesejadas.



(a) Em escala aritmética.

(b) Em escala logarítmica.

Figura 1: Comparação dos métodos de interpolação em relação à quantidade de *shares* (k) utilizada. Fonte: Elaboração própria.

4.4 Análise

O principal questionamento levantado foi se a alteração do método de interpolação poderia melhorar o desempenho computacional do *Shamir Secret Sharing*, considerando que, tradicionalmente, ele é implementado com a interpolação de Lagrange. Além disso, investigou-se de que forma a variação no número de *shares* influenciaria o processo como um todo.

Como todos os métodos de interpolação estão sendo aplicados dentro do corpo finito, não iremos analisar questões de aproximação e arredondamento, tendo em vista que são tratados apenas números inteiros pertencentes ao corpo $\mathbb{Z}_p$.

O comportamento das curvas presente nas Figura 1 está em conformidade com a complexidade teórica prevista para esses métodos, sendo de $O(n^2)$ para interpolação de Lagrange e Newton e $O(n^3)$ para interpolação de Vandermonde. O crescimento mais acentuado é o Vandermonde

(linha verde da Figura 1) porque envolve a resolução de um sistema linear com uma matriz de Vandermonde. Essa matriz pode ser mal-condicionada para grandes graus de polinômio, levando a alta complexidade computacional. Já o crescimento da interpolação de Newton (linha vermelha da Figura 1) ocorre pelo fato de que a interpolação de Newton exige o cálculo de diferenças divididas, cujo custo computacional se torna expressivo em grandes entradas. Por outro lado, a curva correspondente ao métodos de Lagrange, linhas azul da Figura 1, exibem um crescimento mais contido ao longo do aumento do número de *shares*.

A interpolação de Lagrange é amplamente utilizada em *Secret Sharing*, principalmente no *Shamir Secret Sharing*, devido ao bom compromisso entre eficiência e implementação prática em operações modulares. Diferente do método de Newton, que exige um pré-processamento complexo ou armazenamento de coeficientes adicionais, para que possa permitir atualização incremental sem reprocessamento total. Diferente também do método de Vandermonde, que exige a solução de um sistema linear com uma matriz que pode ser computacionalmente intensiva.

5 Considerações Finais

Neste trabalho, mostramos uma análise sobre a alteração do método de interpolação para o esquema criptográfico do *Shamir Secret Sharing*, além de mostrar a influência da alteração na quantidade de *shares* utilizadas no processo. Apresentamos o desempenho computacional e teórico pelo qual se baseia o fato do método de Lagrange ser amplamente utilizado para fins criptográficos, principalmente no contexto de aplicações dentro do corpo finito.

Como trabalhos futuros, pretende-se estender essa metodologia de análise a outros métodos de *Secret Sharing*, como o esquema de Blakey, que se baseia na resolução de sistemas de hiperplanos. Além de expandir tal análise para casos reais, como em sistemas de autenticação de multifatores, privacidade em dados de rede elétrica e afins.

Uma alternativa de estudo para os métodos que apresentaram os piores desempenhos, sobretudo em cenários com grande número de *shares*, é a adoção de técnicas de paralelismo. Acreditamos que, utilizando esta abordagem, podem ser mitigadas e, assim, pode-se otimizar o tempo de processamento, principalmente quando o cenário exige alta demanda computacional.

Agradecimentos

A Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES) e ao Laboratório Nacional de Computação Científica (LNCC) pela infraestrutura, suporte técnico e ambiente científico proporcionado para o desenvolvimento do presente trabalho.

Referências

[1] S. Bezzateev, V. Davydov e A. Ometov. "On secret sharing with newton's polynomial for multi-factor authentication". Em: **Cryptography** 4.4 (2020), p. 34. DOI: 10.3390/cryptography4040034.

[2] R. L. Burden e J. D. Faires. **Numerical Analysis**. 10ª ed. Cengage Learning, 2021. ISBN: 1305253663.

[3] T. R. N. Ferreira. "Modelo criptográfico de múltiplas partes para computação segura de um modelo matemático da transmissão da COVID-19". Dissertação de mestrado. LNCC - Laboratório Nacional de Computação Científica, 2021.

[4] T. Rocha, R. Borseti e F. Borges. "COMPUTAÇÃO SEGURA DE UM MODELO SIR E SIRV". Em: **XXV ENMC – Encontro Nacional de Modelagem Computacional, XIV ECTM – Encontro de Ciência e Tecnologia de Materiais** (2023). DOI: 10.29327/1340957.26-16.

[5] A. Shamir. "How to share a secret". Em: **Communications of the ACM** 22.11 (1979), pp. 612–613. DOI: 10.1145/359168.359176.

