

COMPUTAÇÃO SEGURA DE UM MODELO SIR E SIRV

Thays Rocha[1] - tferreira@posgrad.lncc.br
Renato Borseti[1] - renatojp@posgrad.lncc.br
Fábio Borges[1] - borges@lncc.br
[1]Laboratório Nacional de Computação Científica (LNCC-MCTI) - Petrópolis, RJ, Brasil

Resumo.
Com o objetivo de garantir a integridade e a privacidade de cálculos com dados sensíveis, especialmente em casos em que o cálculo é realizado em máquinas de terceiros ou ambientes inseguros, propusemos o processamento seguro de dois modelos, o SIR (Suscetível-Infectado-Recuperado) e o SIRV (Suscetível-Infectado-Recuperado-Vacinado) da Covid-19 no Brasil, por meio dos Circuitos Aritméticos aplicados ao Método de Múltiplas Partes Shamir Secret Sharing. Demonstramos que o modelo criptográfico proposto é viável para aplicação, visto que os resultados obtidos apresentam similaridade entre o modelo matemático com criptografia e o modelo sem criptografia, apesar do aumento no tempo de processamento.

Keywords: *Shamir Secret Sharing, Modelagem Matemática, Covid-19, Circuitos Aritméticos, Criptografia*

1. INTRODUÇÃO

É indispensável o uso da modelagem matemática para simular cenários e encontrar soluções potenciais para problemas reais. O uso das Equações Diferenciais Ordinárias e Parciais possibilita uma análise mais manuseável de diversos cenários, tornando o processo de resolução mais prático e eficiente, conforme afirma Ferreira et al. (2017).

A área da saúde não é uma exceção, há vários modelos matemáticos para melhor descrever o processo de transmissão de doenças, simulações de previsões de seu comportamento entre outros modelos dentro do que chamamos atualmente de Epidemiologia Matemática. E muitos pesquisadores utilizam máquinas de terceiros que são compartilhadas, tendo em vista que muito destes modelos necessitam de recursos computacionais mais avançados devido a quantidade de dados utilizados.

O grande desafio está em como tratar tais dados, muita das vezes dados pessoais, de forma confidencial em máquinas de terceiros. E é neste cenário emergente que a criptografia se destaca. Dentre os métodos criptográficos existente, podemos citar *Secret Sharing* que é garante a integridade dos dados utilizados. Em junção com Circuitos Aritméticos, podemos garantir também a integridade de operações matemáticas realizadas com tais dados cifrados.

Pesquisas envolvendo a privacidade de dados na área da saúde vem crescendo cada dia mais. Podemos citar, por exemplo, os trabalhos de Ermakova & Fabian (2013); Sarosh et al. (2021); Lakshmi et al. (2021), que utilizam *Secret Sharing* para tal finalidade.

Neste trabalho, apresentamos uma alternativa viável para a computação de operações matemática de forma segura para ambientes externos, muitas vezes considerados inseguros, utilizando o método criptográfico de Múltiplas Partes "Shamir Secret Sharing". Convertemos os modelos de transmissão da Covid-19 descritos no trabalho de Bernine et al. (2020) para Circuitos Aritméticos, a fim de calcularmos de forma homomórfica através do *Shamir Secret Sharing*. Demonstramos se tratar de uma alternativa viável tendo em vista a equivalência dos valores obtidos.

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 do modelo matemático proposto por Bernine et al. (2020) para a transmissão da Covid-19 no Brasil. Na Seção 4, abordamos a aplicação do método criptográfico de Múltiplas Partes *Shamir Secret Sharing* no modelo matemático apresentado anteriormente. Os resultados obtidos e a comparação entre as resoluções realizadas são detalhados na Seção 5. Por fim, na Seção 6, são apresentadas as considerações finais e os interesses referentes a trabalhos futuros.

2. *SHAMIR SECRET SHARING*

Esta seção apresenta os conceitos básicos de *Shamir Secret Sharing* e sua aplicação em Circuitos Aritméticos.

2.1 Conceitos Básicos

No âmbito da criptografia, existe um subcampo conhecido como Computação Segura de Múltiplas Partes, que se concentra em apresentar métodos nos quais a computação é distribuída entre várias partes, sem que elas tenham conhecimento das informações umas das outras. Dentre estes métodos, podemos destacar o *Secret Sharing*, que consiste em particionar um segredo e compartilhar suas partes com os n participantes.

Há duas formas de ocorrer sua reconstrução, ambas necessitando de pelo menos k participantes, com $k < n$. Quando o método possui alguma restrição no conjunto qualificado, ou seja, não é qualquer conjunto de pelo menos k participantes que reconstrói o segredo. Estes casos são denominados métodos que se baseiam em estrutura de acesso. Quando isso não ocorre, ou seja, quando não há restrições, qualquer conjunto de pelo menos k participantes é suficiente para reconstruir o segredo, chamamos de métodos baseados em um limiar.

Para o presente trabalho utilizamos o método baseado em um limiar *Shamir Secret Sharing*, proposto em 1979, com base na literatura (Shamir, 1979). Sendo s o segredo a ser cifrado, n o número total de participantes, k o número mínimo de participantes necessário para reconstrução do segredo e $\mathbb{F}_p$ um corpo finito, com p primo, temos que o segredo s é transformado em polinômio, no qual a parte constante corresponde ao segredo. Em outros termos, temos que é escolhido de forma aleatória valores para $a_i, \forall i \in [1, k-1]$, onde $a_i \in \mathbb{F}_p$ e é definido o polinômio $\mathcal{P}(x) = s + \sum_{i=1}^{k-1} a_i x^i$.

As partições (ou *shares*) a serem compartilhadas com os participantes são os pontos e o valor do polinômio no ponto em questão, ou seja, $\text{Sk}_i = (x_i, \mathcal{P}(x_i) \mod p)$, $\forall i \in [1, n]$. Sua reconstrução se baseia na interpolação de Lagrange sobre Corpos Finitos. Isso ocorre ao utilizar

o conjunto de dados disponível de pelo menos k destes participante para recuperar um único polinômio, $\mathcal{P}'(x)$, de grau $k-1$. A reconstrução é bem-sucedida quando $\mathcal{P}' = \mathcal{P}$ e $\mathcal{P}(0) = s$. Importante destacar que nenhum usuário é capaz de inferir qualquer informação sobre o segredo a partir de sua (*share*) individual.

A metodologia descrita até o momento equivale ao processo de encriptação e decriptação de um segredo. No entanto, quando se deseja executar operações matemáticas de forma criptografada, é necessário utilizar circuitos aritméticos em conjunto com o método de *Shamir Secret Sharing*. Dessa forma, é possível realizar cálculos de maneira segura e protegida, mantendo a confidencialidade das informações envolvidas.

2.2 Circuitos Aritméticos Aplicados ao *Shamir Secret Sharing*

Os circuitos aritméticos realizam as operações aritméticas por meio de portas lógicas, utilizando fios de entrada e saída, todos definidos dentro do contexto do Corpo Finito, de acordo com (SMART, 2016). A Figura 1 representa um exemplo de circuito aritmético, o cálculo da função $f(x) = x_1 \cdot x_2 + x_3 \cdot x_4 \mod p$. Logo, possui três portas lógicas: uma aditiva e duas multiplicativa, além dos fios de entrada, x_1, x_2, x_3 e x_3, e o fio de saída, x_7.

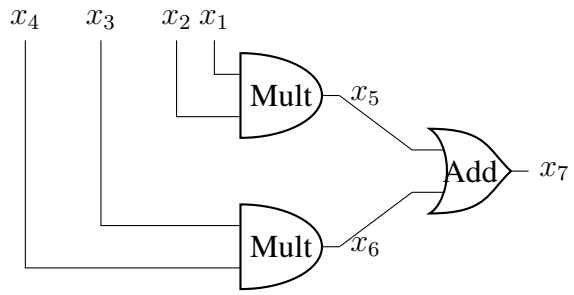

Figura 1: Exemplo de um Circuito Aritmético.

Em 1998, Gennaro apresentou um protocolo, conforme Gennaro et al. (1998), para um Circuito Aritmético que utiliza o *Shamir Secret Sharing*. Esse protocolo possibilita a realização de operações matemáticas de forma criptografada, assegurando assim a privacidade do processo. Mesmo que ocorra uma interceptação ao longo do procedimento, não é possível recuperar os valores reais dos dados utilizados, pois todos estarão cifrados. Dessa maneira, é viável computar a função $f(x_1, x_2, ...)$ definida no corpo $\mathbb{F}_p$, mantendo os valores de x_i como segredos, sem revelar suas informações reais.

3. MODELO MATEMÁTICO

Para demostrar a aplicabilidade do método criptográfico citado anteriormente, no presente trabalho utilizamos os modelos matemáticos descritos no trabalho de Bernine et al. (2020), onde é apresentado dois modelos de análise da propagação da Covid-19 no Brasil, por volta de agosto de 2020. O primeiro cenário simulado foi utilizando o modelo clássico Suscetível-Infectado-Recuperado (SIR). Já para o segundo, foi incluído a classe Vacinados, tornando-se o modelo Suscetível-Infectado-Recuperado-Vacinado (SIRV), devida a relevância da vacina no combate à disseminação de doenças.

Sendo assim, para melhor entendimento do leitor, apresentamos as definições das classes compartimentais utilizadas nos modelos matemáticos, a saber,

- Suscetível (S): Indivíduos que até o momento estão saudáveis e estão aptos a se infectar pelo vírus da doença;
- Infectado (I): Indivíduos que se infectaram com o vírus da doença e podem estar transmitindo-o para os demais;
- Recuperado (R): Indivíduos que se recuperaram da doença e adquiriram imunidade à doença;
- Vacinado (V): Indivíduos que cumpriram o calendário vacinal e, consequentemente, adquiriram imunidade à doença.

Em ambos os cenários, a população total, representada por N, é dada pela soma das classes no tempo t, ou seja, a cada instante de tempo t, cada indivíduo pertence exclusivamente a uma única classe compartimental.

Também é necessário apresentar os parâmetros utilizadas nos modelos matemáticos, que foram definidos da seguinte forma: T tempo total analisado, em dias; α representando a taxa de natalidade brasileira; β representando a taxa de mortalidade das classes não relacionadas à doença; μ representando a taxa de mortalidade pela doença; σ representando a taxa de contágio; γ representando a taxa de recuperação; λ representando a taxa de vacinação; ϵ representando a taxa de indivíduos que perderam a imunidade contra a doença e retornaram à classe Suscetível e são elegíveis para reinfecção da doença.

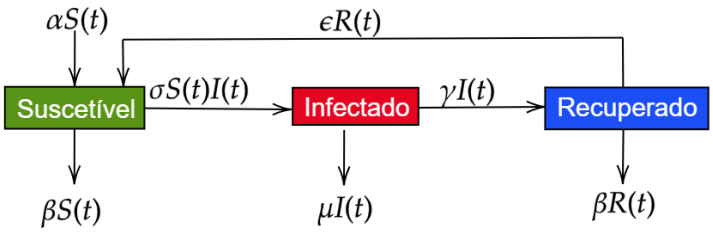

Figura 2: Diagrama das classes compartimentais do modelo SIR.

Os modelos matemáticos foram apresentados em forma de diagramas representando a dinâmica da propagação da doença em cada modelo, SIR e SIRV respectivamente. As Figuras 2 e 3 apresentam tais dinâmicas. É importante destacar que as cores atribuídas a cada classe compartimental nos diagramas serão as mesmas utilizadas no gráfico comparativo ao final deste trabalho.

Entretanto, a Figura 2 pode ser reescrita através do sistema de Equações Diferenciais Ordinárias (EDOs) conforme apresentado abaixo.

$$\begin{cases} \dfrac{dS(t)}{dt} = \alpha S(t) + \varepsilon R(t) - \sigma S(t)I(t) - \beta S(t); \\ \dfrac{dI(t)}{dt} = \sigma S(t)I(t) - \gamma I(t) - \mu I(t); \\ \dfrac{dR(t)}{dt} = \gamma I(t) - \varepsilon R(t) - \beta R(t). \end{cases} \tag{1}$$

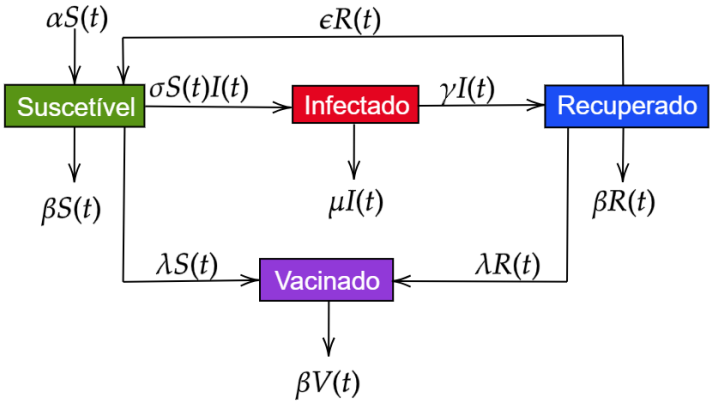

Figura 3: Diagrama das classes compartimentais do modelo SIRV.

Similarmente, a Figura 3 pode ser reescrita através do sistema EDOs apresentado abaixo.

$$\begin{cases} \dfrac{dS(t)}{dt} = \alpha S(t) + \varepsilon R(t) - \sigma S(t)I(t) - \lambda S(t) - \beta S(t); \\ \dfrac{dI(t)}{dt} = \sigma S(t)I(t) - \gamma I(t) - \mu I(t); \\ \dfrac{dR(t)}{dt} = \gamma I(t) - \lambda R(t) - \varepsilon R(t) - \beta R(t); \\ \dfrac{dV(t)}{dt} = \gamma I(t) - \lambda R(t) - \varepsilon R(t) - \beta R(t); \end{cases} \tag{2}$$

A discretização ocorre dividindo o intervalo $[0, T]$ em m subintervalos espaçados de tamanho $\Delta t = \frac{T}{m}$. Desta forma, temos que $[0, T] = [t_0, t_1] \cup [t_1, t_2] \cup \cdots \cup [t_{m-1}, t_m]$. Para aproximas as derivas de primeira ordem das funções S, I, R e V, foi utilizado o método numérico de Diferenças Finitas Regressivas, uma vez que é conhecido por ser um método incondicionalmente estável, conforme Richard et al. (2015). Sendo assim, a Equação (1) é expressa da seguinte forma:

$$\begin{cases} (1 - \alpha\Delta t + \beta\Delta t)S_i = \varepsilon R_{i-1}\Delta t + (1 - \sigma I_{i-1}\Delta t)S_{i-1}; \\ (1 + \gamma\Delta t + \mu\Delta t)I_i = (1 + \sigma S_{i-1}\Delta t)I_{i-1}; \\ (1 + \beta\Delta t)R_i = \gamma I_{i-1}\Delta t + (1 - \varepsilon\Delta t)R_{i-1}. \end{cases} \tag{3}$$

Assim como a Equação (2) é expressa da seguinte forma:

$$\begin{cases} (1-\alpha\Delta t+\beta\Delta t)S_i &= \varepsilon R_{i-1}\Delta t+(1-\sigma I_{i-1}\Delta t)S_{i-1}; \\ (1+\gamma\Delta t+\mu\Delta t)I_i &= (1+\sigma S_{i-1}\Delta t)I_{i-1}; \\ (1+\lambda\Delta t+\beta\Delta t)R_i &= \gamma I_{i-1}\Delta t+(1-\varepsilon\Delta t)R_{i-1}; \\ (1+\beta\Delta t)V_i &= \lambda\Delta t(S_i+R_i)+V_{i-1}. \end{cases} \tag{4}$$

4. APLICAÇÃO DO *SHAMIR SECRET SHARING* AO MODELO PROPOSTO

Com o objetivo de realizar o cálculo dos modelos matemáticos propostos por Bernine et al. (2020) de maneira criptografada, utilizamos Circuito Aritmético aplicado ao *Shamir Secret Sharing*, conforme descrito anteriormente. Para isso, utilizamos um cenário em que há cinco pessoas participantes do processo, em que há a necessidade da união de pelo menos três destas cinco para poder realizar o cálculo e revelar seu resultado. A ideia de baseia na contextualização de um representante por região do país, tendo em vista que os modelos estão analisando todo o país, ou seja, terá um representante da região Sul, Sudeste, Norte, Nordeste e Centro-Oeste.

No entanto, o cenário fica a critério do pesquisador que utilizará esse método, permitindo que o mesmo o adapte de acordo com a situação que melhor se adequar à sua problemática específica. Com tudo, dependendo do tamanho de n, seu tempo de processamento se torna inviável para utilização, já que seus crescimentos ocorrem de forma proporcional. Considerando todas essas informações, cabe ao pesquisador avaliar até que ponto essa metodologia é benéfica para seus objetivos específicos.

Foram considerados 13 valores como segredos, dos quais 8 correspondem aos parâmetros utilizados no modelo, 4 se referem às classes compartimentais empregadas e 1 está relacionado ao valor 1 utilizado em várias etapas do modelo matemático. O corpo utilizado foi $\mathbb{F}_p$, com o número primo $p \approx 2^{128}$.

Entretanto, devido a aritmética modular necessário para o método criptográfico, é necessário utilizar artifícios que transforme os dados necessários para o modelo matemático em valores inteiros positivos. Para isso, foi utilizado a representação do ponto fixo, que consiste em representar a parte inteira de um número com precisão adicional de y casas decimais, onde y é o valor da precisão desejada. Essa abordagem possibilita utilizar os valores decimais que, de outra forma, seriam truncados, permitindo uma representação mais precisa e detalhada dos dados.

A Figura 4 é a representação do Circuito Aritmético referente a classe compartimental Suscetível do modelo SIR, conforme a Equação (3). De forma similar, foi realizado um Circuito Aritmético para cada uma das classes compartimentais, em cada um dos modelos descritos anteriormente, tanto o SIR, quanto o SIRV.

Em relação às portas lógicas utilizadas, recorremos à negação de um dos fios de entrada na porta lógica aditiva para efetuar a subtração necessária do modelo. Entretanto, o resultado de tal subtração deve pertencer ao Corpo Finito utilizado. Caso contrário, o valor a ser decifrado será um valor aleatório, tendo em vista que estará fora do domínio em questão.

O fio de saída descrito com "*up*" representa o cálculo do numerador da equação. Assim como, o fio de saída descrito com "*down*" representa o cálculo do denominador da equação.

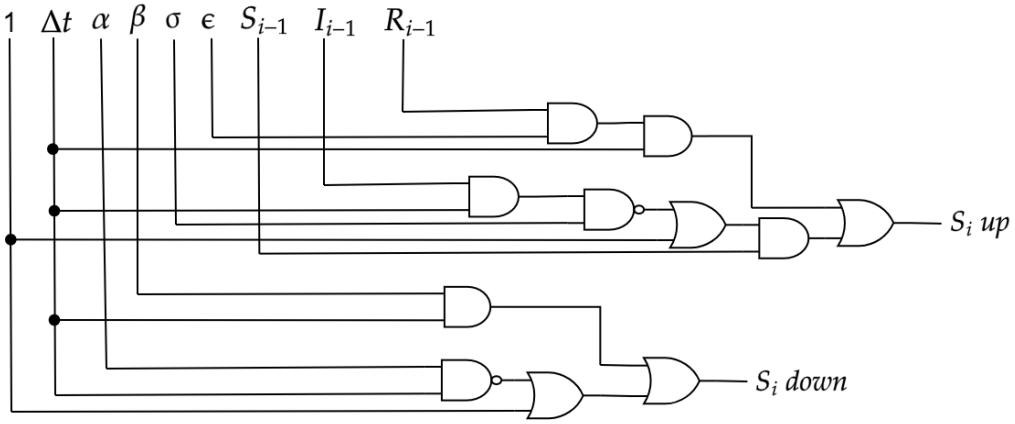

Figura 4: Circuito Aritmético para a classe compartimental S_i do modelo SIR.

Entretanto, há uma limitação no método criptográfico proposto quanto estamos trabalhando com a operação da divisão. É possível realizar tal operação de forma cifrada, desde que seja garantido que seu resultado seja um inteiro positivo, devido à necessidade de pertencer ao Corpo Finito. Para estes casos, calculamos a inversa do denominador através do teorema de Fermat ou do algoritmo de Euclides, por exemplo.

É valido frisar que o código foi criado na linguagem *Python* versão 3.8, através do *Integrated Development Environment* (IDE) (Ambiente de Desenvolvimento Integrado, em português) Spyder, em uma máquina com processador Intel Core i3, com 4GB de RAM e com sistema operacional Ubuntu, versão 22.04.

5. RESULTADOS E DISCUSSÕES

Para a resolução dos modelos matemáticos propostos no trabalho de Bernine et al. (2020), os valores utilizados, tanto para os parâmetros quanto para as classes compartimentais mencionados anteriormente, estão disponíveis na Tabela 1 abaixo. Os resultados estão apresentados nos gráficos das Figuras 5 e 6, referentes aos modelos SIR e SIRV, respectivamente.

Tabela 1: Dados utilizados para a simulação.

Parâmetros	Valor	Cond. Inic.	Valor
α	38488050×10^{-12}	S(0)	205721209
β	17045917×10^{-12}	I(0)	858376
μ	170846×10^{-9}	R(0)	2947250
γ	4208943×10^{-9}	V(0)	0
σ	1171255×10^{-16}		
ε	5502466×10^{-12}		
λ	1916916×10^{-9}		
T	800		

Como o objetivo é demonstrar a similaridade dos valores obtidos no cálculo de forma cifrada e não cifrada, optamos por representar graficamente ambos os métodos juntos, sobrepondo seus

resultados. Com isso, temos que as linhas contínuas presentes nos gráficos indicam que foram valores obtidos de forma cifrada, utilizando o método criptográfico descrito anteriormente. Já as linhas pontilhadas, um pouco mais claras, indicam que foram obtidas de forma tradicional, sem criptografia.

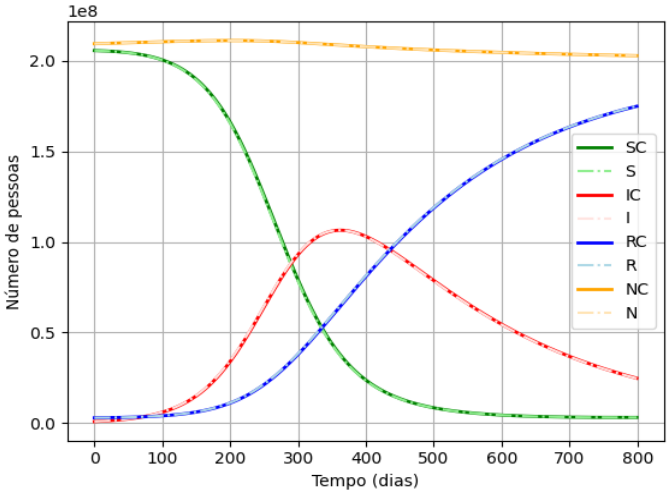

Figura 5: Gráfico sobreposto referente ao modelo cifrado e não cifrado do modelo SIR.

Na legenda presente em ambos os gráficos, das Figuras 5 e 6, foi acrescentada a letra "**C**" a cada classe para indicar que a classe correspondente foi calculada de forma cifrada. Ou seja, "**S**" representa o resultado do cálculo da classe Suscetíveis e "**SC**" representa a classe Suscetíveis de forma criptografada; "**I**" indica a classe Infectados e "**IC**" indica a classe Infectados de forma criptografada; "**R**" corresponde à classe Recuperados e "**RC**" corresponde à classe Recuperados de forma criptografada; "**V**" representa a classe Vacinados e "**VC**" representa a classe Vacinados de forma criptografada; e, por fim, "**N**" é utilizado para o cálculo da população total e "**NC**" é utilizado para o cálculo da população total de forma criptografada.

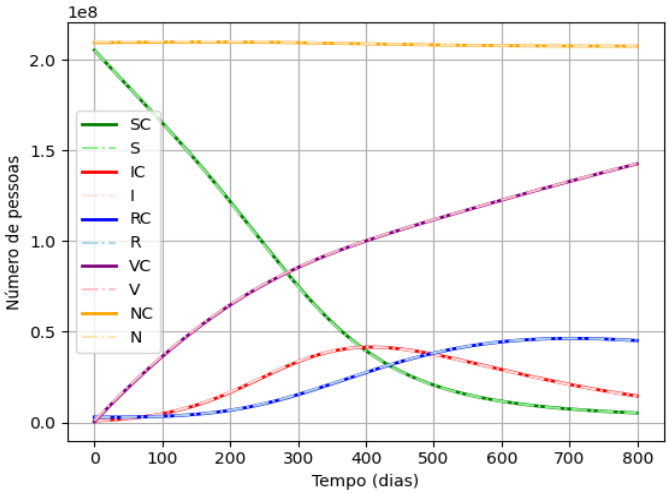

Figura 6: Gráfico sobreposto referente ao modelo cifrado e não cifrado do modelo SIRV.

Dessa forma, ao analisar as Figuras 5 e 6 podemos concluir que o modelo criptografado

proposto é válido, uma vez que os resultados obtidos são similares nos modelos SIR e SIRV, com discrepância mínima, devido ao truncamento dos valores durante a conversão de números em ponto flutuante para números inteiros. Notavelmente, o comportamento de cada uma das curvas que representa as classes compartimentais permanece o mesmo, independentemente de terem sido calculadas de forma cifrada ou não. Isso demonstra a eficácia e a consistência do método criptográfico aplicado à resolução dos modelos matemáticos.

A Tabela 2 abaixo apresenta o tempo de processamento, em segundos, de cada modelo, SIR e SIRV, e a forma em que foi calculada, cifrada ou não. Na forma cifrada, apresentamos todas as variações possíveis do método proposto, ou seja, com a união de três pessoas, com a união de quatro pessoas e a com a união das cinco pessoas.

Tabela 2: Análise do tempo de execução de cada modelo.

Modelo	Não Cifrado	Cifrado (3,5)	Cifrado (4,5)	Cifrado (5,5)
SIR	$\approx 1.16825e-5$	≈ 2.03217	≈ 3.500229	≈ 4.42319
SIRV	$\approx 1.38282e-5$	≈ 2.59342	≈ 4.65566	≈ 5.60998

É notório que ocorra um crescimento, mesmo que pequeno, do tempo de processamento dependendo da quantidade de pessoas utilizadas no processo de decriptação dos modelos matemáticos. Esse aumento ocorre devido ao acréscimo de dados necessários para tal processamento. Isso é esperado quando aumentamos o n.

6. CONCLUSÃO

Neste trabalho, mostramos uma alternativa viável para computação segura de dados em um ambiente externo, que em sua maioria das vezes é inseguro. Apresentamos uma opção para realização de operações matemáticas, através do método criptográfico de Múltiplas Partes *Shamir Secret Sharing*. Com ele, tanto os dados utilizados quanto o cálculo são realizados de forma cifrada, a fim de proteger a integridade e a privacidade do processo, respectivamente.

Como pode ser visto, o modelo criptográfico proposto se torna válido tendo em vista a similaridade dos valores obtidos em comparação com os valores obtidos no cálculo sem a criptografia, mesmo com um aumento do tempo de processamento. No entanto, ao ponderar o aumento do tempo de processamento em relação à segurança e privacidade dos dados utilizados no processo, constata-se que o desempenho do modelo criptográfico proposto é satisfatório. Portanto, consideramos essa alternativa viável para todos que necessitam processar seus dados sensíveis em computadores compartilhados, priorizando sua proteção.

Como trabalhos futuros, há o interesse em aplicar essa metodologia em problemas de grande porte, especialmente na área de *Internet of Things* (IoT). Além disso, abre-se espaço para explorar formas de otimização do método, bem como a aplicação de outros métodos para computação segura de múltiplas partes, permitindo, assim, uma comparação entre eles.

Agradecimentos

A CAPES pelo apoio para o desenvolvimento do presente trabalho.

Referências

Bernine, E., Rocha, T., Pereira, D. e Borges, F., (2020), "Cenário após a vacinação da população brasileira contra a Covid-19 através da Modelagem Matemática", *XXIII ENMC – Encontro Nacional de Modelagem Computacional e XI ECTM – Encontro de Ciências e Tecnologia de Materiais*, Palmas, TO.

Ermakova, T., e Fabian, B.(2013)." Secret sharing for health data in multi-provider clouds",*2013 IEEE 15th conference on business informatics*, p. 93-100.

Ferreira, T. R. N. and Mesquita, F. H. e Telles, W. R. (2017). "Simulação do transporte de contaminantes em rios utilizando o método de volumes finitos", *Encontro Nacional de Modelagem Matemática e Encontro de Ciência e Tecnologia de Materiais*, Nova Friburgo, RJ.

Gennaro, R., Rabin, M. O., e Rabin, T. (1998). "Simplified VSS and fast-track multiparty computations with applications to threshold cryptography". In *Proceedings of the seventeenth annual ACM symposium on Principles of distributed computing*, p. 101-111.

Lakshmi, V. S., Deepthi, S., e Deepthi, P. P. (2021). "Collusion resistant secret sharing scheme for secure data storage and processing over cloud",*Journal of Information Security and Applications*, v. 60, p. 102869.

Richard, L., Burden, J., Faires, D. e Burden, A., (2015), "*Análise Numérica*", 3ª ed., Cengage Learning, São Paulo.

Sarosh, P., Parah, S. A., Bhat, G. M., Heidari, A. A., e Muhammad, K (2021). " Secret sharing-based personal health records management for the Internet of Health Things",*Sustainable Cities and Society*, v. 74, p. 103129.

Shamir, A. (1979), "How to share a secret." *Communications of the ACM*, v.22, n.11, p.612-613.

Smart, P. N. "Cryptography made simple". Springer International Publishing Switzerland, 2016.

SECURE COMPUTATION OF AN SIR AND SIRV MODEL

Abstract. *To guarantee the integrity and privacy of negotiations with sensitive data, especially in cases where the calculation is performed on third-party machines or insecure environments, we proposed the secure processing of two models, the SIR (Susceptible-Infected-Recovered) and the SIRV (Susceptible-Infected-Recovered-Vaccinated) of Covid-19 in Brazil, through the Arithmetic Circuits applied to the Shamir Secret Sharing Multipart Method. We demonstrate that the standard cryptographic model is viable for application, since the results obtained show similarity between the mathematical model with encryption and the model without encryption, despite the increase in processing time.*

Keywords: *Shamir Secret Sharing, Mathematical Modeling, Covid-19, Arithmetic Circuits, Cryptography*