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

Explorando Grafos e Estruturas Algébricas na Segurança Criptográfica

Leonardo B. de Souza[1]
Centro Federal de Educação Tecnológica Celso Suckow da Fonseca, Rio de Janeiro, RJ
Augusto Parisot[2], Vitor S. Ponciano[3], Rafael Oliveira[4]
Centro de Análises de Sistemas Navais, Rio de Janeiro, RJ

Resumo. Na era da computação quântica, a segurança da informação torna-se um desafio crescente, uma vez que muitos algoritmos criptográficos tradicionais podem se tornar vulneráveis a ataques quânticos. Diante disso, é essencial investigar novas abordagens para o desenvolvimento de criptografia pós-quântica, explorando ferramentas matemáticas que possam garantir segurança mesmo na presença de computadores quânticos. Uma abordagem muito promissora nesse campo é o estudo de grafos associados a estruturas algébricas. Para cada grupo finito, por exemplo, é possível relacioná-lo a diferentes classes de grafos. As propriedades estruturais desses grafos refletem a natureza do grupo, oferecendo uma nova perspectiva para o desenvolvimento da teoria. Nosso objetivo é explorar a interação entre teoria dos grafos e estruturas algébricas para esquemas criptográficos baseado em grupos algébricos, capaz de oferecer resistência contra ataques quânticos.

Palavras-chave. Criptografia Pós-Quântica, Teoria dos Grafos, Grupos Algébricos

1 Introdução

A palavra "criptografia"encontra suas raízes no grego antigo, unindo "kryptós"(escondido) e "gráphein"(escrever), o que já nos indica a arte de escrever de forma oculta. No universo da segurança digital, a criptografia assume um papel central ao converter dados legíveis em um formato cifrado. Sua robustez é fundamental para a proteção de dados, sendo o método primordial e indispensável para prevenir o acesso indevido a informações em sistemas computacionais, bloqueando sua leitura ou exploração mal-intencionada.

Um dos pilares da criptografia moderna é o sistema RSA. Nele, as chaves pública e privada são definidas por pares de números naturais, (e, n) e (d, n), respectivamente. O número n é obtido pela multiplicação de dois números primos. A segurança do RSA reside na dificuldade de se obter a chave privada a partir da pública, o que equivale a encontrar os fatores primos do número n. Ao selecionar cuidadosamente esses dois primos, essa fatoração se torna um problema computacionalmente árduo [2]. Desde 1994, com o trabalho do matemático Peter Shor, que introduziu algoritmos quânticos aplicáveis a problemas de fatoração de inteiros e logaritmos discretos [4], ficou evidente que o advento dos computadores quânticos poderia potencialmente expor a vulnerabilidade do RSA.

Esquemas criptográficos que resistem a ataques quânticos são conhecidos como *pós-quânticos*. Com o objetivo de acelerar a implementação desses esquemas, o Instituto Nacional de Padrões e Tecnologia (NIST) iniciou um processo de padronização em [1]. Esse processo foca em primitivas

[1]oelsouza.math@gmail.com
[2]parisot@marinha.mil.br
[3]vtponciano@gmail.com
[4]rafael-silva.oliveira@marinha.mil.br

 © 2026 SBMAC

essenciais para comunicação segura na Internet, incluindo assinaturas digitais e troca de chaves. Este artigo propõe uma modificação de criptossistema simétrico baseado em grafos proposto por [3], onde modificamos a estrutura algébrica visando fornecer confidencialidade de dados entre remetente e destinatário em ambientes de comunicações seguras.

O texto está organizado em seções. Na Seção 2, exploramos o conceito de grafos direcionados e estruturas algébricas, criando uma operação que forma um grupo abeliano. Na Seção 3, utilizamos essas estruturas de grupo no grafo para desenvolver um sistema criptográfico simétrico. A Seção 4 apresenta uma análise detalhada do sistema criptográfico simétrico proposto. Por fim, na Seção 5, apresentamos as conclusões obtidas a partir deste estudo.

2 Estrutura Algébrica Proposta para Grafos

Esta seção apresenta uma estrutura algébrica proposta para grafos finitos, onde os grafos são definidos por conjuntos de vértices e arestas direcionadas, e uma operação binária chamada $\otimes$ é definida para combinar grafos. A operação $\otimes$ é definida com base em quatro tipos de arestas base, representando diferentes direções de conexão entre os vértices. Em seguida, são demonstradas propriedades fundamentais dessa operação, incluindo fechamento, associatividade, identidade e inverso, para mostrar que o conjunto de grafos com a operação $\otimes$ formam um grupo.

Seja $G = (V, E)$ um grafo finito e direcionado, com:

$$V(G) = \{v_1, v_2, \ldots, v_n\} \text{ e } E(G) = \{e_1, e_2, \ldots, e_m\} \cup \{e'_1, e'_2, \ldots, e'_m\}. \tag{1}$$

tal que $e_k = (v_i, v_j)$ e $e'_k = (v_j, v_i)$, onde i e $j \in [1, n]$ e $k \in [1, m]$. Dizemos que um grafo é direcionado quando cada aresta possui um sentido, para simplificação omitiremos o v, de modo que $e = (v_i, v_j) = (i, j)$. Podemos definir as direções como um conjunto base de arestas do tipo $[e_k, e'_k] = B_\ell$, $0 \leq \ell \leq 3$, tal que:

$$\begin{aligned} B_0 &= [(\emptyset, \emptyset), (\emptyset, \emptyset)] && \text{sem aresta} \\ B_1 &= [(i, j), (\emptyset, \emptyset)] && \text{unidirecional} \\ B_2 &= [(\emptyset, \emptyset), (j, i)] && \text{unidirecional} \\ B_3 &= [(i, j), (j, i)] && \text{bidirecional.} \end{aligned} \tag{2}$$

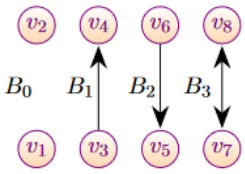

Figura 1: As arestas da base. Fonte: Dos autores.

Dados dois grafos simples direcionados G e H de ordem n, iremos definir uma operação binária denotada por $\otimes$ definida em G e H, de modo que $\mathcal{G} = G \otimes H$ é o grafo resultante de ordem n, tal que $|V(\mathcal{G})| = |V(G)| = |V(H)| = n$, e para o conjunto de arestas $E(\mathcal{G})$, a pertinência de uma aresta base B em $\mathcal{G}$ é determinada usando as relações da Tabela 1.

Cada grafo é representado pelo conjunto de arestas da combinação das arestas bases da Figura 1, indicados na Tabela 1 a seguir.

Note que:

$$E(G_m) = [[e_1, e'_1], [e_2, e'_2], [e_3, e'_3], \ldots, [e_m, e'_m]] = [B_{a_1}, B_{a_2}, \ldots, B_{a_m}]. \tag{3}$$

 © 2026 SBMAC

Tabela 1: Relações entre as arestas bases B_0, B_1, B_2 e B_3 dos grafos $\mathcal{G}, G$ e H.

$\otimes$	G_{B_0}	G_{B_1}	G_{B_2}	G_{B_3}
H_{B_0}	$\mathcal{G}_{B_0}$	$\mathcal{G}_{B_1}$	$\mathcal{G}_{B_2}$	$\mathcal{G}_{B_3}$
H_{B_1}	$\mathcal{G}_{B_1}$	$\mathcal{G}_{B_0}$	$\mathcal{G}_{B_3}$	$\mathcal{G}_{B_2}$
H_{B_2}	$\mathcal{G}_{B_2}$	$\mathcal{G}_{B_3}$	$\mathcal{G}_{B_0}$	$\mathcal{G}_{B_1}$
H_{B_3}	$\mathcal{G}_{B_3}$	$\mathcal{G}_{B_2}$	$\mathcal{G}_{B_1}$	$\mathcal{G}_{B_0}$

Aqui, $a_i \in \{0, 1, 2, 3\}$, onde $0 \leq i \leq m$. Na Figura 2, é indicado um exemplo de operação com dois grafos.

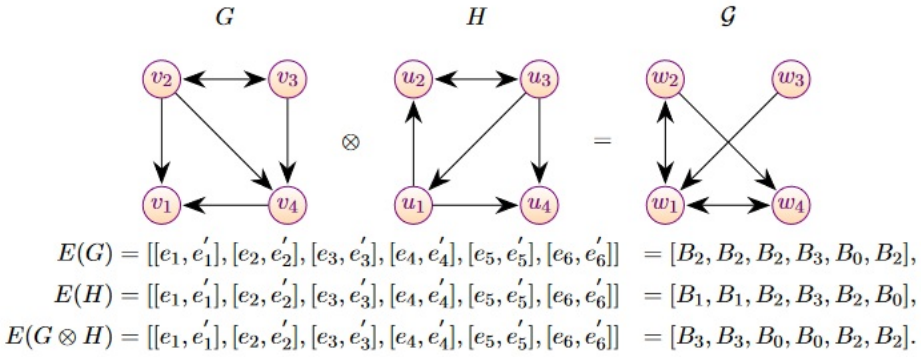

Figura 2: Exemplo da operação entre dois grafos. Fonte: Dos autores.

Teorema 1: Seja G^n o conjunto de grafos finitos de ordem n. Junto com a operação $\otimes$ definida na Tabela 1, $\langle G^n, \otimes \rangle$ é um grupo.

Prova: Para provar que $\langle G^n, \otimes \rangle$ é um grupo, a operação $\otimes$ deve satisfazer as seguintes propriedades:

- **P.1** A operação $\otimes$ obedece à propriedade de fechamento sobre G^n.
- **P.2** A operação $\otimes$ obedece à propriedade associativa sobre os elementos de G^n.
- **P.3** Existe um elemento identidade, digamos $G_I \in G^n$, tal que para cada grafo $G_x \in G^n$ satisfaz:

$$G_I \otimes G_x = G_x \otimes G_I = G_I. \tag{4}$$

- **P.4** Para cada elemento $G_x \in G^n$, existe um elemento inverso $G'_x \in G^n$ tal que:

$$G_x \otimes G'_x = G'_x \otimes G_x = G_I. \tag{5}$$

Teorema 2.1. *A operação $\otimes$ obedece à propriedade de fechamento.*

Demonstração. De acordo com a definição de $\otimes$, para quaisquer dois grafos G_x e G_y de alguma ordem n, $G_x \otimes G_y$ também é um grafo de ordem n com $V(G_x \otimes G_y) = V(G_x) = V(G_y)$. Como G^n consiste em todos os grafos de ordem n, $G_x \otimes G_y \in G^n$. Portanto, a propriedade de fechamento é verdadeira. □

DOI: 10.5540/03.2026.012.01.0286

© 2026 SBMAC

Teorema 2.2. *A operação $\otimes$ obedece à propriedade associativa.*

Para quaisquer três grafos G_x, G_y e G_z de ordem n, a seguinte condição é verdadeira:

$$(G_x \otimes G_y) \otimes G_z = G_x \otimes (G_y \otimes G_z). \tag{6}$$

Demonstração. Para demonstrar essa igualdade para o conjunto de elementos em G^n, é crucial considerar operações em todas as condições possíveis da Tabela 1, conforme evidenciado na Tabela 2. É importante notar que o número de permutações possíveis para testar a associatividade é de 64 possibilidades, porém, em nossa demonstração, consideramos apenas 8 casos, uma vez que, como podemos observar na Tabela 1, as operações são comutativas.

Tabela 2: Resultados da propriedade associativa da operação $\otimes$.

G_x	G_y	G_z	$(G_x \otimes G_y) \otimes G_z$	$G_x \otimes (G_y \otimes G_z)$
B_0	B_0	B_0	B_0	B_0
B_0	B_0	B_1	B_1	B_1
B_0	B_0	B_2	B_2	B_2
B_0	B_0	B_3	B_3	B_3
B_0	B_1	B_2	B_3	B_3
B_0	B_1	B_3	B_2	B_2
B_0	B_2	B_3	B_1	B_1
B_1	B_2	B_3	B_0	B_0

□

Teorema 2.3. *Existência do elemento identidade em G^n com relação à operação $\otimes$.*

Demonstração. O grafo $G_\emptyset$, com $V(G_\emptyset) = n$ e $E(G_\emptyset) = \{B_0, B_0, ..., B_0\}$, é o elemento identidade em relação à operação $\otimes$. Isso ocorre porque, para qualquer grafo $G_a \in G^n$:

$$G_x \otimes G_\emptyset = G_\emptyset \otimes G_x = G_x. \tag{7}$$

□

Teorema 2.4. *Existência do elemento inverso em G^n com relação à operação $\otimes$.*

Demonstração. Um grafo G com n vértices é complementado ao grafo $\overline{G}$, definido da seguinte forma: $V(\overline{G}) = V(G)$, $e \in E(\overline{G}) \iff e \notin E(G)$. Em outras palavras, $\overline{G}$ contém exatamente as arestas que não estão em G.

O grafo G_{K_n}, com $V(G_{K_n}) = n$ e $E(G_{K_n}) = \{B_3, B_3, \ldots, B_3\}$, é o elemento utilizado como unidade em relação à operação $\otimes$. Isso ocorre porque, para qualquer grafo $G_x \in G^n$:

$$G_x \otimes \overline{G}_x = \overline{G}_x \otimes G_x = G_{K_n}. \tag{8}$$

□

Logo, a propriedade acima é verdadeira para $\otimes$ sobre G^n. Portanto, pelas propriedades demonstradas nos Teoremas anteriores, temos que $\langle G^n, \otimes \rangle$ é um grupo.

Teorema 2.5. *$\langle G^n, \otimes \rangle$ é abeliano.*

Prova: Para provar a afirmação acima, é necessário mostrar que $\langle G^n, \otimes \rangle$ é um grupo e $\otimes$ obedece à lei comutativa, como provado pela Tabela 1.

DOI: 10.5540/03.2026.012.01.0286 © 2026 SBMAC

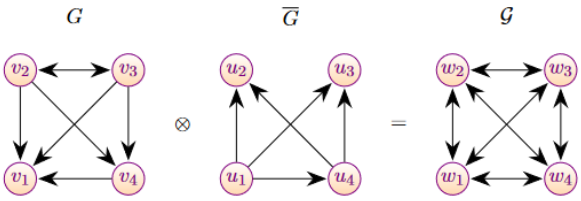

Figura 3: Exemplo da operação grafo inverso, onde $E(G) = [B_1, B_2, B_1, B_2, B_1, B_2, B_3, B_0]$ e $E(\overline{G}) = [B_2, B_1, B_2, B_1, B_2, B_1, B_0, B_3]$. Fonte: Dos autores.

3 Sistema Cripto-Simétrico Proposto Baseado em $\langle G^n, \otimes \rangle$

Nesta seção, apresentamos o sistema cripto-simétrico proposto baseado em $\langle G^n, \otimes \rangle$. A criptografia simétrica é um método de criptografia onde a mesma chave é usada tanto para criptografar quanto para descriptografar uma mensagem. Isso significa que o remetente e o destinatário da mensagem compartilham a mesma chave secreta. Nas próximas seções vamos definir o nosso processo criptográfico.

3.1 Selecionando o valor de n

No primeiro passo, a ordem do grafo é selecionada. Isso, por sua vez, define o conjunto $\langle G^n \rangle$ e o grupo abeliano $\langle G^n, \otimes \rangle$.

3.2 Selecionando a Chave Secreta G_s e G'_s

Um grafo de $\langle G^n \rangle$ é selecionado aleatoriamente como a chave de criptografia secreta, denotado por G_s. Assume-se que o grafo G_s é compartilhado secretamente entre o remetente e o receptor, seguindo as propriedades da chave simétrica. O receptor, ao conhecer o grafo G_s, pode facilmente gerar o grafo inverso G'_s de G_s. O grafo nulo e o grafo completo de ordem n não são selecionados como chave porque o grafo nulo é o elemento identidade e o grafo completo é o complemento do nulo.

3.3 Mapeamento do Texto Plano para o Grafo de Texto Plano G_P

Neste passo, o texto plano é convertido em um grafo de texto plano G_P de ordem n. Existem várias maneiras de gerar o grafo de texto plano. A abordagem mais simples deste processo é demonstrada pelo Algoritmo 1. Neste processo, o texto plano é convertido em seu formato binário equivalente. Suponha que o comprimento de P no formato binário seja n_P. No segundo passo, a sequência binária é dividida em blocos de n bits e atribuída a uma matriz $n \times n$ de baixo para cima. Como $n_P \leq n^2$, os bits restantes $n^2 - n_P$ nas linhas superiores são preenchidos com zeros. A matriz final é o grafo de texto plano de P. O processo reverso do Algoritmo 1 pode ser seguido para gerar o texto plano P a partir de G_P.

DOI: 10.5540/03.2026.012.01.0286

© 2026 SBMAC

Input: Texto plano P
Output: Grafo de texto plano G_P

1. Converter P em sua string binária $bin(P)$;
2. Deixar $n_P =$ comprimento de $bin(P)$;
3. Dividir $bin(P)$ em blocos de comprimento n;
4. Criar uma matriz de adjacência de $n \times n$;
5. Alocar blocos de n bits de $bin(P)$ da direita para a esquerda, na matriz de adjacência de baixo para cima;
7. Preencher com zeros nas linhas superiores para tornar múltiplo de n^2;
8. A matriz correspondente é o grafo de texto plano G_P;

3.4 Criptografia do Grafo de Texto Plano

O processo de criptografia é definido por:

$$G_C = G_P \otimes G_K. \tag{9}$$

onde G_C é o grafo do texto cifrado. Em outras palavras, o grafo do texto cifrado é gerado aplicando a operação $\otimes$ nos grafos G_P e G_K.

3.5 Descriptografia do Grafo do Texto Cifrado

Durante o processo de descriptografia, o grafo do texto plano original é gerado pela seguinte operação:

$$G_P = G_C \otimes G'_s. \tag{10}$$

Ou seja, a operação $\otimes$ é realizada no grafo do texto cifrado G_C e no grafo da chave inversa G'_s para produzir G_P. O processo acima é demonstrado com um exemplo a seguir. Suponha que $n = 4$ e o texto plano $P = 202$. Então, $P = (11001010)_2$ em formato binário. A matriz de adjacência do grafo de texto plano G_P para o texto plano P é dada por:

$$G_P = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \end{pmatrix}. \tag{11}$$

onde, a $3^{\underline{a}}$ e $4^{\underline{a}}$ linhas contêm P na ordem de cima para baixo, e as duas linhas restantes ($1^{\underline{a}}$ e $2^{\underline{a}}$ linha) da matriz consistem em zeros preenchidos. A correção e a análise do sistema cripto proposto são fornecidas.

4 Análise

Nesta seção, primeiro a correção do sistema cripto proposto é verificada. Depois, sua força de segurança é analisada contra ataques de força bruta. Para verificar a correção do sistema cripto proposto, é necessário mostrar que as operações usadas para os processos de criptografia e descriptografia podem gerar com sucesso o texto plano a partir do texto cifrado.

Teorema 4.1. *Para quaisquer grafos G_P e G_s em G^n, se G'_s é o grafo inverso de G_s em G^n, então:*

$$G_P = ((G_P \otimes G_s) \otimes G'_s) \otimes G_{K_n}. \tag{12}$$

DOI: 10.5540/03.2026.012.01.0286 © 2026 SBMAC

Demonstração.

$$\begin{aligned}((G_P \otimes G_s) \otimes G'_s) \otimes G_{K_n} &= (G_P \otimes (G_s \otimes G'_s)) \otimes G_{K_n} \quad \text{(P.1 } \otimes\text{)} \\ &= (G_P \otimes G_{K_n}) \otimes G_{K_n} \quad \text{(P.3 } \otimes\text{)} \\ &= G'_P \otimes G_{K_n} = G_P.\end{aligned} \tag{13}$$

□

4.1 Resiliência Contra Ataque de Força Bruta

Considere G_C e o valor de n. Sem informação adicional, são necessárias $O(n^2 \cdot 2^{n^2})$ operações para encontrar o valor do grafo chave G_s.

Prova: Sem informação adicional, o processo de criptoanálise deve tentar a abordagem de força bruta para encontrar G_s. Para encontrar G_s usando força bruta, é necessário tentar todos os $G_i \in G_m$ para verificar se $G_i \otimes G_C$ resulta em um texto plano significativo. Dado n, tentar todas as chaves envolve $O(2^{n^2})$ operações. Em segundo lugar, a operação $\otimes$ requer $O(n^2)$ operações. Portanto, são necessárias no total $O(n^2 \cdot 2^{n^2})$ operações para encontrar o grafo chave G_s. Para um valor suficientemente grande de n, $O(2^{n^2})$ é computacionalmente difícil com um dispositivo de computação padrão.

5 Considerações Finais

Neste trabalho, exploramos a interseção entre grafos e estruturas algébricas como uma abordagem inovadora para aprimorar a segurança criptográfica na era da computação quântica. Através do estudo detalhado dos grafos associados a grupos finitos, como os obtidos a partir das tabelas de Cayley, identificamos que uma compreensão aprofundada dessas estruturas pode ser fundamental para o desenvolvimento de algoritmos criptográficos robustos.

Propomos uma nova operação binária, denotada por $\otimes$, para combinar grafos direcionados, e demonstramos que, com essa operação, o conjunto de todos os grafos de uma ordem fixa forma um grupo. A utilização de grafos como representações de chaves e textos criptográficos apresenta uma estrutura flexível e resistente, que pode ser adaptada para responder às ameaças emergentes da computação quântica.

Referências

[1] L. Chen, S. Jordan, Y.-K. Liu, D. Moody, R. Peralta, R. Perlner e D. Smith-Tone. **Report on Post-Quantum Cryptography**. Rel. técn. U.S. Department of Commerce, National Institute of Standards e Technology, 2016.

[2] J. Hoffstein, J. Pipher e J. H. Silverman. **An Introduction to Mathematical Cryptography**. Vol. 1. Springer, 2008.

[3] A. K. Mishra, B. K. Singh e R. Misra. "Graph-Based Symmetric Crypto-System for Data Confidentiality". Em: **Proceedings of the 2018 IEEE Global Communications Conference (GLOBECOM)**. IEEE, 2018, pp. 1–6.

[4] P. W. Shor. "Algorithms for Quantum Computation: Discrete Logarithms and Factoring". Em: **Proceedings of the 35th Annual Symposium on Foundations of Computer Science**. IEEE, 1994, pp. 124–134.

 © 2026 SBMAC