Criptografia Homomórfica

Daniel Muller Rezende[1]

[1]Instituto de Ciência da Computação– Universidade Federal de Juiz de Fora (UFJF)
Juiz de Fora – MG – Brazil

daniel.rezende@estudante.ufjf.br

Abstract. *Homomorphic encryption is a crucial area of information system security, enabling operations on encrypted data without the need for decryption. With this in mind, this paper addresses the main concepts, types, and algorithms involved in this type of encryption. Furthermore, performance tests were conducted, as well as the main use cases for these algorithms were explored.*

Resumo. *Criptografia homomórfica é uma área muito importante da segurança em sistemas de informação, através da qual é possível realizar operações sobre dados criptografados sem a necessidade de descriptografá-los. Tendo isso em vista, este trabalho busca abordar os principais conceitos, tipos e algoritmos envolvidos neste tipo de criptografia. Além disso, foram realizados testes de desmpenho, bem como a exploração dos principais casos de uso destes algoritmos.*

1. Introdução

A criptografia homomórfica (HE) é uma técnica criptográfica avançada que permite que operações computacionais sejam realizadas sobre dados criptografados sem a necessidade de decifrá-los, garantindo assim a confidencialidade dos dados [Moore et al. 2014], [Tourky et al. 2016]. Ao contrário da criptografia tradicional, que exige a decifração dos dados antes do processamento, expondo-os a potenciais riscos de segurança durante a computação, a criptografia homomórfica estende a segurança às operações de processamento de dados, preservando a confidencialidade durante todo o processo. Essa capacidade é particularmente valiosa em ambientes de computação em nuvem, onde os dados devem ser processados por servidores remotos ou provedores de serviços não confiáveis sem revelar seu conteúdo original.

A HE surgiu como uma solução promissora para os desafios de segurança e privacidade de dados no cenário computacional moderno. A ideia de computar em dados criptografados foi proposta pela primeira vez em 1978, mas permaneceu um problema em aberto e um desafio de pesquisa por décadas. No entanto, avanços significativos transformaram a HE em um poderoso instrumento para aprimorar a segurança de dados. Ela facilita a computação que preserva a privacidade, a terceirização segura de tarefas computacionais e a análise colaborativa de dados em diversas indústrias, como finanças e saúde, sem comprometer a privacidade das informações sensíveis.

2. Tipos de criptografia homomórfica

A criptografia homomórfica (HE) é classificada em diferentes categorias, dependendo das capacidades de computação que oferece sobre dados cifrados, sem a necessidade

de decifrá-los. Essas classificações refletem o nível de funcionalidade e as restrições inerentes a cada tipo de esquema, abordando os desafios de segurança e privacidade em ambientes como a computação em nuvem.

A Criptografia Parcialmente Homomórfica (PHE) é o primeiro tipo de HE criado, que suporta apenas um único tipo de operação homomórfica sobre dados criptografados, seja adição ou multiplicação. Isso significa que, se um esquema for aditivamente homomórfico, ele permitirá somas de valores cifrados que, quando decifrados, corresponderão à soma dos valores originais. Da mesma forma, um esquema multiplicativamente homomórfico permitirá apenas operações de multiplicação. Exemplos clássicos de PHE incluem o esquema Paillier, que é aditivamente homomórfico, e o RSA (sem preenchimento), que é multiplicativamente homomórfico.

Em um nível intermediário, encontra-se a Criptografia Semi-Homomórfica (SHE). Este tipo de esquema é mais avançado que a PHE, pois suporta um número limitado de operações homomórficas, incluindo tanto adição quanto multiplicação sobre dados cifrados. No entanto, a SHE possui restrições significativas quanto à quantidade de operações sequenciais ou à profundidade do circuito que pode ser avaliada antes que o ruído inerente ao processo criptográfico se acumule a ponto de impedir uma decifração correta. Apesar dessas limitações, a SHE representa um passo importante em direção à HE completa, ao permitir uma gama mais ampla de computações.

Por fim, a Criptografia Totalmente Homomórfica (FHE) é considerada o "Santo Graal"da criptografia por sua capacidade de realizar quaisquer computações arbitrárias e ilimitadas em dados cifrados, sem a necessidade de decifrá-los. A ideia de computar sobre dados criptografados foi proposta inicialmente em 1978, mas foi somente em 2009 que Craig Gentry apresentou o primeiro esquema plausível de FHE, revolucionando o campo da criptografia. A FHE permite que organizações terceirizem o processamento de dados para a nuvem ou para serviços não confiáveis, garantindo a confidencialidade das informações durante todo o ciclo de vida computacional. Apesar de ser a forma mais poderosa de HE, a FHE ainda enfrenta desafios relacionados ao custo computacional elevado e à complexidade de implementação, embora pesquisas contínuas busquem otimizações para torná-la mais prática para aplicações em tempo real.

3. Principais algoritmos

Esta seção é responsável por descrever os principais algoritmos de criptografia homomórfica que foram implementados neste trabalho. Dentre eles, será descrito o funcionamento do RSA, Paillier e CKKS.

3.1. Rivest-shamir-adleman (RSA)

O RSA é um dos primeiros métodos de criptografia de chave pública e foi proposto em 1978. Ele também possui uma propriedade homomórfica. O funcionamento do RSA começa com a geração de chaves, onde são selecionados dois números primos aleatórios grandes, p e q. A partir deles, calcula-se:

$$n = p \times q, \tag{1}$$

$$\phi(n) = (p-1) \times (q-1) \tag{2}$$

Em seguida, um número inteiro e é escolhido de modo que seja relativamente primo a $\phi(n)$. Por fim, d é dado por:

$$d = 1(mod(\phi(n))) \tag{3}$$

A chave pública é composta por n, e, e a chave privada por n, d. Para cifrar uma mensagem M (que deve ser menor que n), calcula-se o texto cifrado C como:

$$C = M^e mod(n) \tag{4}$$

Para decifrar o texto cifrado C, a mensagem original M é recuperada calculando:

$$M = C^d mod(n) \tag{5}$$

Uma característica importante do RSA é ser um criptosistema multiplicativamente homomórfico. Isso significa que, ao multiplicar dois textos cifrados, $C1$ e $C2$, o resultado após a decifração será o produto das mensagens originais $M1 \times M2$.

3.2. Esquema paillier

O esquema de criptografia Paillier é um algoritmo de chave pública probabilístico. Sua base matemática reside na suposição de resíduo composto, onde um número n é o produto de dois grandes números primos p e q escolhidos aleatoriamente. Para a geração de chaves, primeiro são selecionados dois números primos grandes, p e q, a partir dos quais se calcula:

$$n = p \times q \tag{6}$$

A chave pública é então composta por g, n, onde g é um inteiro aleatório. Para cifrar uma mensagem M, que deve ser um número menor que n, o texto cifrado C é gerado utilizando a equação:

$$C = g^M * r^n mod(n^2), \tag{7}$$

em que r é um número aleatório selecionado.

A decifração do texto cifrado C permite a recuperação da mensagem original M a partir da equação:

$$M = L(g^\lambda mod(n^2)) \times \mu mod(n), \tag{8}$$

Uma característica fundamental do Paillier é ser um criptosistema aditivamente homomórfico. Isso significa que, dadas apenas a chave pública e as cifragens de duas mensagens, $M1$ e $M2$, é possível computar uma nova cifragem que, ao ser decifrada, revelará a soma das mensagens originais $M1 + M2$. Essa propriedade permite realizar somas em dados criptografados sem a necessidade de decifrá-los. Por suportar exclusivamente operações de adição, o Paillier é classificado como um tipo de Criptografia Parcialmente Homomórfica (PHE).

3.3. Cheon-Kim-Kim-Song (CKKS)

O esquema CKKS (Cheon–Kim–Kim–Song), proposto por [Cheon et al. 2017], é um algoritmo de criptografia homomórfica voltado para cálculos sobre números reais ou complexos aproximados. Diferente de outros esquemas que operam apenas sobre inteiros exatos, o CKKS introduz um método de codificação que representa números de ponto flutuante como coeficientes de um polinômio, aplicando uma escala fixa para preservar a precisão. Essa abordagem permite que operações como somas e multiplicações sejam executadas diretamente sobre os dados criptografados, com resultados também na forma criptografada, sem a necessidade de descriptografia intermediária. A grande vantagem do CKKS é viabilizar computações complexas de forma segura, mesmo em ambientes não confiáveis, com tolerância a pequenos erros numéricos.

No funcionamento geral, a criptografia no CKKS transforma o vetor de valores reais em um polinômio codificado, que é então embaralhado utilizando a chave pública e parâmetros criptográficos definidos para garantir segurança contra ataques conhecidos. Durante as operações homomórficas, o esquema controla fatores como escala (para manter precisão), profundidade multiplicativa (quantidade de multiplicações consecutivas antes de precisar de reescalonamento) e modulação dos coeficientes (para administrar o ruído gerado). Na descriptografia, o polinômio resultante é recombinado com a chave secreta para recuperar o polinômio codificado original, e então decodificado para retornar uma aproximação dos valores reais iniciais. Esse design torna o CKKS ideal para aplicações de aprendizado de máquina, análise estatística e processamento de sinais sobre dados sensíveis.

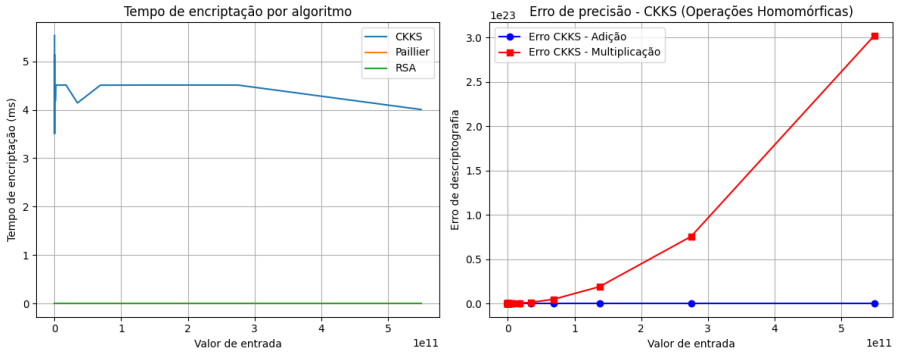
4. Avaliação de desempenho

A parte prática deste trabalho consistiu em avaliar duas métricas de dsempenho dos algoritmos implementados. A primeira avaliou o tempo necessário para encriptação em cada algoritmo e a segunda avaliou o acúmulo de ruído durante as operações de multiplicação e adição no algoritmo CKKS. Para isso, os algoritmos foram testados em uma sequência de números inteiros vairando de 1 a 10^{11}.

Na Figura 1, o primeiro hgráfico compara os tempos de encriptação dos algoritmos CKKS, Paillier e RSA. Nele é possível observar que o CKKS apresenta tempos significativamente maiores que os outros dois algoritmos, mantendo-se na faixa de aproximadamente 4 a 5 ms, com pequenas variações à medida que o valor de entrada aumenta. Já o RSA e o Paillier mostram tempos praticamente nulos na escala apresentada, sugerindo que, para o conjunto de valores testados, esses algoritmos realizam a encriptação de forma mais rápida que o CKKS. Essa diferença de desempenho é esperada, já que o CKKS é um esquema de criptografia homomórfica aproximada, mais complexo e custoso computacionalmente, enquanto o RSA e o Paillier não lidam com operações sobre dados encriptados de maneira tão intensiva.

No segundo gráfico, que avalia o erro de precisão no CKKS para operações homomórficas de adição e multiplicação, percebe-se que a adição cresce linearmente a uma taxa significativamente baixa. Já a multiplicação apresenta um crescimento exponencial no erro à medida que o valor de entrada aumenta, atingindo magnitudes muito altas para valores grandes. Esse comportamento reflete uma característica fundamental do CKKS: enquanto adições possuem um comportamento linear preservando melhor a pre-

Figura 1. Métricas de desempenho.



cisão, multiplicações sucessivas amplificam o ruído inerente à codificação aproximada, o que pode comprometer a acurácia de cálculos após certo número de operações. Isso reforça a necessidade de técnicas como reescalonamento (rescaling) ou gerenciamento cuidadoso de profundidade computacional para manter resultados úteis.

5. Casos de Uso

A criptografia homomórfica (HE) oferece uma variedade de aplicações essenciais no cenário digital atual, especialmente onde a confidencialidade dos dados é primordial e a computação em ambientes não confiáveis é necessária. Seu principal benefício reside na capacidade de realizar operações computacionais diretamente sobre dados criptografados sem a necessidade de decifrá-los, garantindo assim a privacidade da informação durante todo o ciclo de processamento. A HE, portanto, surge como uma solução para os desafios de segurança e privacidade que surgem quando os dados são transferidos para servidores remotos ou ambientes de rede leve.

Um dos principais casos de uso da criptografia homomórfica é a análise de dados que preserva a privacidade. Esta técnica permite que cálculos sejam realizados em dados sensíveis sem expor o conteúdo original, o que é crucial em cenários onde múltiplas partes precisam colaborar na análise de informações confidenciais sem revelá-las.

No setor da saúde, a criptografia homomórfica faz uma contribuição significativa ao abordar a necessidade de análise e compartilhamento de informações de saúde de forma segura e com privacidade [Roumpies and Kakarountas 2023]. Médicos, pesquisadores e instituições podem realizar computações em prontuários de pacientes criptografados para análises complexas, pesquisa colaborativa e medicina personalizada, tudo isso sem comprometer a privacidade individual ou violar regulamentações rigorosas.

A HE também se estende a outras áreas emergentes, como a Internet das Coisas (IoT) e ambientes leves, onde aprimora as capacidades de comunicação, garantindo privacidade e segurança dos dados [Ullah et al. 2024]. Isso inclui aplicações em casas inteligentes seguras, IoT de saúde e IoT industrial, onde os dados dos sensores são criptografados antes da transmissão e processamento. No setor financeiro, além da análise de tendências, a criptografia homomórfica é empregada para proteger transações sensíveis e dados de consumidores, facilitando a detecção de fraudes e análises eficientes [Agarwal and Shrivastava 2021]. Por fim, a HE possibilita aplicações criptografadas de ponta a ponta, como mensagens seguras e serviços bancários, onde a privacidade dos

dados do usuário é mantida durante todo o processo computacional sem sacrificar a funcionalidade. Mesmo em tecnologias como o blockchain, a HE pode ser utilizada para garantir a verificação segura de transações e a auditoria com preservação da privacidade.

6. Conclusões

A criptografia homomórfica (HE) representa uma inovação fundamental no campo da criptografia, permitindo que operações computacionais sejam realizadas diretamente sobre dados cifrados, sem a necessidade de decifrá-los, garantindo assim a confidencialidade da informação. Por sua capacidade de preservar a privacidade dos dados durante o processamento em ambientes não confiáveis, como a computação em nuvem, a HE é frequentemente referida como o "Santo Graal"da criptografia.

Apesar do seu imenso potencial, a criptografia homomórfica ainda enfrenta desafios significativos, principalmente relacionados ao custo computacional elevado e à complexidade de implementação. As operações em dados criptografados são consideravelmente mais lentas do que em dados em texto simples, e o gerenciamento seguro das chaves de criptografia é uma tarefa complexa. Contudo, a pesquisa contínua tem se concentrado na otimização de algoritmos e no desenvolvimento de aceleração por hardware para tornar a HE mais prática e eficiente. À medida que a tecnologia avança, a criptografia homomórfica está cada vez mais próxima de permitir interações digitais verdadeiramente seguras e privadas, com aplicações transformadoras em áreas como IoT, inteligência artificial, saúde, e sistemas financeiros, prometendo um futuro onde a privacidade e o progresso tecnológico coexistam.

Referências

Agarwal, P. and Shrivastava, P. (2021). Enhancing data security in cloud computing through homomorphic encryption. *Comput. J. Appl. Comput. Sci. Intell. Technol*, 1(1):32–39.

Cheon, J. H., Kim, A., Kim, M., and Song, Y. (2017). Homomorphic encryption for arithmetic of approximate numbers. In *International conference on the theory and application of cryptology and information security*, pages 409–437. Springer.

Moore, C., O'Neill, M., O'Sullivan, E., Doröz, Y., and Sunar, B. (2014). Practical homomorphic encryption: A survey. In *2014 IEEE International Symposium on Circuits and Systems (ISCAS)*, pages 2792–2795. IEEE.

Roumpies, F. and Kakarountas, A. (2023). A review of homomorphic encryption and its contribution to the sector of health services. In *Proceedings of the 27th Pan-Hellenic Conference on Progress in Computing and Informatics*, pages 237–242.

Tourky, D., ElKawkagy, M., and Keshk, A. (2016). Homomorphic encryption the "holy grail" of cryptography. In *2016 2nd IEEE International Conference on Computer and Communications (ICCC)*, pages 196–201. IEEE.

Ullah, S., Chen, J. L. J., Ali, I., Khan, S., Hussain, M. T., Ullah, F., and Leung, V. C. (2024). Homomorphic encryption applications for iot and light-weighted environments: A review. *IEEE Internet of Things Journal*.