Análise de confiabilidade dos algoritmos de criptografia

Giullio E da C Di Gerolamo[1]

[1]Departamento de Computação – Universidade Federal de São Carlos (UFSCar)
São Carlos – SP – Brazil

Resumo. *A crescente digitalização da sociedade tem aumentado a necessidade de manter a segurança das comunicações e dados sensíveis. A criptografia é o método pelo qual isso é feito. No entanto, a confiabilidade e a eficácia dos algoritmos de criptografia estão em risco devido aos constantes avanços tecnológicos e ameaças cibernéticas. É fundamental garantir que os sistemas de criptografia permaneçam fortes e capazes de resistir a ataques potenciais. Em resumo, o objetivo da pesquisa proposta é examinar os elementos essenciais que afetam a confiabilidade dos algoritmos de criptografia em face de ameaças emergentes, contribuindo para a proteção contínua dos dados digitais e promovendo a segurança cibernética global.*

Abstract. *The growing digitization of society has increased the need to maintain the security of communications and sensitive data. Encryption is the method by which this is achieved. However, the reliability and effectiveness of encryption algorithms are at risk due to constant technological advancements and cyber threats. It is crucial to ensure that encryption systems remain robust and capable of withstanding potential attacks. In summary, the aim of the proposed research is to examine the essential elements affecting the reliability of encryption algorithms in the face of emerging threats, contributing to the ongoing protection of digital data and promoting global cybersecurity.*

1. Introdução

Na sociedade contemporânea, a crescente digitalização tem produzido uma revolução profunda e abrangente, que se estende por todos os aspectos da vida moderna. A capacidade de comunicar, compartilhar e armazenar informações de maneira instantânea e global trouxe consigo inúmeras vantagens, desde avanços na eficiência até a promoção da colaboração em escala global. No entanto, essa nova era de interconexão também trouxe desafios e ameaças sem precedentes, destacando a importância crítica da segurança cibernética.

Nesse contexto, a criptografia emerge como uma salvaguarda vital para as comunicações e dados sensíveis, fornecendo uma camada de proteção que visa manter a confidencialidade e a integridade das informações em trânsito. Através de algoritmos matematicamente complexos, a criptografia busca tornar os dados ilegíveis para qualquer pessoa não autorizada que possa interceptá-los, garantindo que apenas os destinatários designados possam acessar e compreender o conteúdo.

No entanto, a eficácia a longo prazo da criptografia está constantemente sob ameaça. O ritmo acelerado da inovação tecnológica tem permitido que hackers e atores maliciosos explorem novas brechas e vulnerabilidades em sistemas de segurança aparentemente robustos. Além disso, o advento da computação quântica apresenta um desafio ainda mais formidável à criptografia tradicional, ameaçando a segurança dos sistemas atuais.

Portanto, a necessidade de analisar a confiabilidade dos algoritmos de criptografia torna-se imperativa. O objetivo central deste estudo é conduzir uma análise profunda das nuances que afetam a confiabilidade desses algoritmos diante das ameaças emergentes. Por meio de uma abordagem minuciosa, este artigo busca identificar os pontos fortes e fracos dos métodos de criptografia, levando em consideração tanto os avanços tecnológicos quanto as tendências de ataques cibernéticos. Ao entender os fatores que podem comprometer a eficácia da criptografia, a pesquisa visa contribuir para a identificação de soluções e estratégias que permitam fortalecer a segurança dos dados digitais no futuro.

Existem vários métodos de análise de confiabilidade dos algoritmos de criptografia, sendo os mais comuns: testes de penetração, análise de código e revisão por pares. Os testes de penetração envolvem tentativas de invadir o sistema para identificar vulnerabilidades. A análise de código é uma revisão detalhada do código-fonte em busca de erros ou fraquezas. Já a revisão por pares envolve uma equipe de especialistas que avalia o código e identifica possíveis problemas.

Assim, a jornada em direção a um entendimento mais profundo da confiabilidade dos algoritmos de criptografia não apenas ilumina os desafios presentes e futuros da segurança cibernética, mas também fornece um alicerce crucial para a proteção contínua das informações em uma era digital em constante evolução.

2. Trabalhos Relacionados

O Portal de Periódicos CAPES realizou uma pesquisa bibliográfica usando os termos de busca "criptografia", "algoritmos" e "confiabilidade". A pesquisa não teve nenhum resultado, mas ao pesquisar os mesmos termos em inglês, descobriu mais de 940 artigos relevantes. Para melhorar a busca, a string adicional "segurança" em inglês também foi usada, reduzindo o número de artigos mostrados. Isso permite que a pesquisa chegue mais perto do objetivo, que é analisar a confiabilidade dos algoritmos de criptografia e como eles se relacionam com a velocidade.

Diversos artigos científicos foram examinados durante a busca por compreender a confiabilidade dos algoritmos de criptografia e fatores que podem afetar a mesma. Esses artigos também contribuíram para a estruturação do presente estudo. O artigo "A RISC-V Post Quantum Cryptography Instruction Set Extension for Number Theoretic Transform to Speed-Up CRYSTALS Algorithms" é um dos trabalhos escolhidos (P. Nannipieri, S. Di Matteo, L. Zulberti, F. Albicocchi, S. Saponara and L. Fanucci, 2021). Este estudo considerou a escolha de utilização de criptografia quântica e novas

tecnologias pós computação quântica, porém estas novas tecnologias demandam recursos computacionais não negligenciáveis a serem executados. No estudo foi testado trocar na relação complexidade e performance para executar os algoritmos baseados em reticulados CRYSTALS-Kyber e -Dilithium introduziu-se uma Unidade Lógica Aritmética dedicada pós-quântica, incorporada diretamente no pipeline de um processador RISC-V.

O estudo "Um estudo passo a passo dos algoritmos de Grover e Shor" (VIEIRA, L. A.; ALBUQUERQUE, C. D. de, 2023) também aborda o estudo da computação quântica; no entanto, utilizando os algoritmos Grover e Shor que são duas das principais descobertas da computação quântica no início das pesquisas nessa área. O primeiro é um algoritmo de busca com um ganho de velocidade significativo em relação aos algoritmos clássicos e com grande aplicação na resolução de diversos outros problemas. O segundo é capaz de resolver o problema da fatoração de um número C em tempo polinomial, o que foi responsável por um grande impulso na pesquisa em computação e criptografia quântica. Nesse estudo teve como objetivo entender o passo a passo de cada um desses algoritmos e a aplicação das portas quânticas e a percepção das propriedades quânticas.

O estudo de Andrade, R. S., & Silva, F. dos S. (2012) “Algoritmo de criptografia RSA: análise entre a segurança e velocidade”, mostra uma visão mais antiga devido ao seu ano de pesquisa ser a mais de 10 anos atrás, porém também acrescenta para a análise em pauta presente neste artigo, mostrando uma relação entre segurança e velocidade de codificação e decodificação do algoritmo de criptografia RSA, que utiliza um par de números inteiros como ‘chave’. Observando o tempo de processamento em função do tamanho das chaves, confrontando segurança e desempenho.

O estudo "Early Soft Error Reliability Analysis on RISC-V" (N. Lodéa et al., 2022) fez uma análise da arquitetura utilizada no processador RISC-V, muito usada para programar algoritmos de criptografia devido ao seu padrão aberto e à arquitetura de conjunto de instruções livre. Nesse artigo propõe-se uma avaliação antecipada de confiabilidade contra soft errors de um processador RISC-V, estendendo o framework de injeção de falhas SOFIA previamente proposto. Resultados de 850 mil injeções de falhas mostram que a escolha da flag do compilador -O2 para otimizar o desempenho provoca 96% mais falhas de travamento (Hang) do que -O0. Este trabalho auxilia engenheiros de software a desenvolver sistemas e algoritmos de criptografia baseados em RISC-V com tolerância a falhas de maneira mais eficiente.

Finalmente, o artigo "An improvement of both security and reliability for elliptic curve scalar multiplication Montgomery algorithm" (Bedoui, M., Bouallegue, B., Mestiri, H. et al., 2023) aborda uma nova proposta de detecção de falhas baseada em redundância de tempo para o algoritmo de Multiplicação Escalar de Curva Elíptica de Montgomery. Dividiu-se o projeto ECC(Elliptic curve cryptosystems) em três blocos com registradores posicionados entre eles. Quando comparada ao algoritmo de Montgomery ECSM original, a solução deles ocupa cerca de 11,65% a mais de recursos (slices), mas proporciona um ganho de frequência de 51,27%. Para que assim melhorar sua vulnerabilidade a ataques físicos com o objetivo de obter a chave secreta, apesar de sua segurança.

Esses estudos fornecem uma visão abrangente dos vários métodos utilizados para avaliar e melhorar assim como otimizar os diversos algoritmos de criptografia apresentados e amplamente utilizados na área da segurança de dados tanto hoje em dia quanto num passado próximo, importante ressaltar que cada um destes métodos são específicos para suas respectivas tecnologias apresentadas, visando sempre a melhora do estudo apresentado como objetivo.

3. References

P. Nannipieri, S. Di Matteo, L. Zulberti, F. Albicocchi, S. Saponara and L. Fanucci, "A RISC-V Post Quantum Cryptography Instruction Set Extension for Number Theoretic Transform to Speed-Up CRYSTALS Algorithms," in IEEE Access, vol. 9, pp. 150798-150808, 2021, doi: 10.1109/ACCESS.2021.3126208. Disponível em: https://ieeexplore.ieee.org/document/9605604

VIEIRA, L. A.; ALBUQUERQUE, C. D. de. Um estudo passo a passo dos algoritmos de Grover e Shor. C.Q.D. - Revista Eletrônica Paulista de Matemática, Bauru, v. 19, 2020. Disponível em: https://sistemas.fc.unesp.br/ojs/index.php/revistacqd/article/view/278

ANDRADE, Rafael Santos; SILVA, Fernando dos Santos. Algoritmo de criptografia RSA: análise entre a segurança e velocidade. Eventos Pedagógicos, [S. l.], v. 3, n. 3, p. 438–457, 2012. DOI: 10.30681/reps.v3i3.9329. Disponível em: https://periodicos.unemat.br/index.php/reps/article/view/9329

N. Lodéa et al., "Early Soft Error Reliability Analysis on RISC-V," in IEEE Latin America Transactions, vol. 20, no. 9, pp. 2139-2145, Sept. 2022, doi: 10.1109/TLA.2022.9878169. Disponível em: https://ieeexplore.ieee.org/document/9878169

Bedoui, M., Bouallegue, B., Mestiri, H. et al. An improvement of both security and reliability for elliptic curve scalar multiplication Montgomery algorithm. Multimed Tools Appl 82, 11973–11992 (2023). Disponível em: https://link.springer.com/article/10.1007/s11042-022-13749-4#