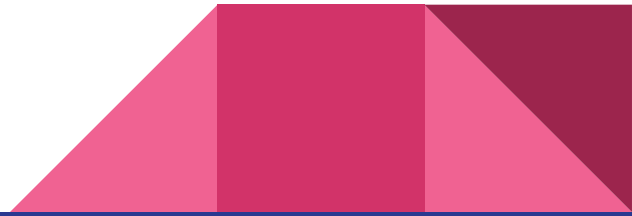
Análise de confiabilidade dos algoritmos de criptografia

Giullio Emmanuel da Cruz Di Gerolamo - 790965

- Introdução
- O que é criptografia?
- Objetivo de pesquisa
- Hipótese de pesquisa
- Artigos Relacionados
- Conclusão



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.

O que é criptografia?

Nesse cenário, a criptografia surge como uma defesa vital para informações sensíveis, protegendo a confidencialidade e integridade dos dados em trânsito. Utilizando algoritmos complexos, ela visa tornar dados ilegíveis para intrusos, permitindo apenas acesso aos destinatários autorizados. Contudo, a eficácia a longo prazo é desafiada pelo ritmo veloz da inovação, abrindo brechas para ataques maliciosos, inclusive pela ameaça crescente da computação quântica sobre sistemas de segurança.

Objetivo de pesquisa:Por que é importante analisar a confiabilidade dos algoritmos de criptografia?

Assim, é vital examinar a confiabilidade dos algoritmos de criptografia. Este estudo visa analisar profundamente como esses algoritmos são afetados por ameaças emergentes. Através de uma análise minuciosa, busca-se identificar os pontos fortes e fracos da criptografia, considerando avanços tecnológicos e tendências em ataques cibernéticos. Compreender os fatores que prejudicam a eficácia da criptografia é crucial para encontrar soluções e estratégias que fortaleçam a segurança dos dados digitais no futuro.

Hipótese de pesquisa:
Para melhorar um aspecto de um algoritmo, é necessario um sacrifício

Existem vários métodos de melhorar um algoritmo de criptografia, dentre eles a otimização .é sempre a resposta mais comum, porém a hipótese apresentada é de que todos esses métodos carregam junto a ti algum custo, seja ele em hardware ou em algum aspecto do próprio software.

Artigos Relacionados

Artigo 1

O artigo "A RISC-V Post Quantum Cryptography Instruction Set Extension for Number Theoretic Transform to Speed-Up CRYSTALS Algorithms" examina o uso de criptografia quântica e novas tecnologias pós-computação quântica, que demandam recursos computacionais significativos. O estudo testou a troca entre complexidade e desempenho ao executar os algoritmos CRYSTALS-Kyber e -Dilithium baseados em reticulados. Uma Unidade Lógica Aritmética pós-quântica foi incorporada diretamente no pipeline de um processador RISC-V para otimizar a execução dos algoritmos.

Artigo 2

O estudo "Um estudo passo a passo dos algoritmos de Grover e Shor" (VIEIRA, L. A.; ALBUQUERQUE, C. D. de, 2023) explora os algoritmos Grover e Shor na computação quântica. O algoritmo de Grover otimiza buscas em comparação com abordagens clássicas, tendo amplas aplicações. Já o algoritmo de Shor resolve a fatoração de números de forma eficiente, impulsionando a pesquisa em criptografia e computação quântica. O estudo visa a compreensão detalhada desses algoritmos, incluindo a aplicação de portas quânticas e propriedades quânticas subjacentes.

Artigo 3

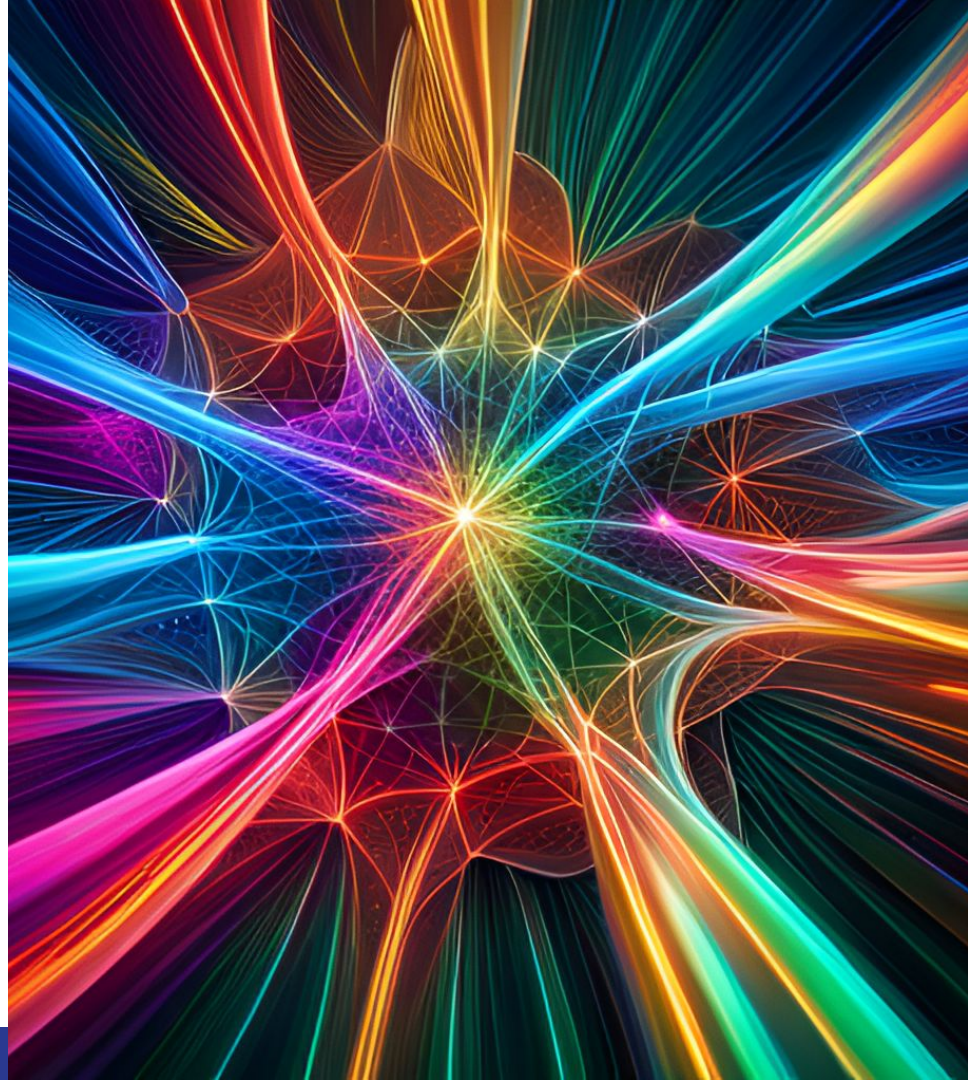
O estudo de Andrade, R. S., & Silva, F. dos S. (2012) "Algoritmo de criptografia RSA: análise entre a segurança e velocidade", embora tenha mais de 10 anos, contribui para a análise atual. Ele examina a relação entre a segurança e a velocidade do algoritmo de criptografia RSA, que emprega um par de números inteiros como chave. Ao avaliar o tempo de processamento em relação ao tamanho das chaves, o estudo aborda o equilíbrio entre segurança e desempenho.

Artigo 4

O estudo "Early Soft Error Reliability Analysis on RISC-V" (N. Lodéa et al., 2022) analisou a arquitetura do processador RISC-V, comumente usada para algoritmos de criptografia devido à sua natureza de código aberto. O artigo propôs avaliar a confiabilidade contra erros suaves em um processador RISC-V, expandindo um framework de injeção de falhas chamado SOFIA. Os resultados de 850 mil falhas mostraram que otimizar o desempenho com a flag de compilação -O2 causou 96% mais falhas de travamento (Hang) do que -O0. Isso ajuda engenheiros de software a criar sistemas e algoritmos de criptografia mais robustos em RISC-V.

Artigo 5

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) apresenta uma nova abordagem de detecção de falhas para o algoritmo de Multiplicação Escalar de Curva Elíptica de Montgomery. Dividindo o projeto ECC (Elliptic curve cryptosystems) em três blocos com registradores intermediários, a solução melhora a frequência em 51,27% com um aumento de recursos de 11,65%, em relação ao algoritmo ECSM original de Montgomery. Isso tem o propósito de elevar a segurança e confiabilidade do algoritmo, tornando-o mais resistente a ataques físicos que visam a obtenção da chave secreta, apesar de sua segurança intrínseca.



Conclusão

Concluindo

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 e que todos carregam um preço como apresentado na hipótese da pesquisa.

Referências

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

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

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

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#